

## RECHTBANK DEN HAAG

Team handel

zaaknummer / rolnummer: C/09/455237 / HA ZA 13-1325

**Vonnis van 23 juli 2014**

in de zaak van

1. **BART THEOPHILUS NOOITGEDAGT**,  
(hierna: Nooitgedagt),  
wonende te Amsterdam,
2. **BRENNO JOHAN SIMON AYMARD AUGUST FRANS DE WINTER**,  
(hierna: De Winter),  
wonende te Ede,
3. **JOHANNES CORNELIS VAN BEEK**,  
(hierna: Van Beek),  
wonende te Amsterdam,
4. **ROBERT VALENTIJN GONGGRIJP**,  
(hierna: Gonggrijp),  
wonende te Amsterdam,
5. **MATHIEU HENDRIK PAAPST**,  
(hierna: Paapst),  
wonende te Siddeburen,
6. De vereniging **NEDERLANDSE VERENIGING VOOR STRAFRECHTADVOCATEN**,  
(hierna: de NVSA),  
gevestigd te Goirle,
7. De vereniging **NEDERLANDSE VERENIGING VOOR JOURNALISTEN**,  
(hierna: de NVJ),  
gevestigd te Amsterdam,
8. De vereniging **INTERNET SOCIETY NEDERLAND**,  
(hierna: Internet Society Nederland),  
gevestigd te Den Haag,
9. De stichting **STICHTING PRIVACY FIRST**,  
(hierna: Privacy First),  
gevestigd te Amsterdam,  
eisers,  
advocaat mr. Chr.A. Alberdingk Thijm te Amsterdam,

tegen

**DE STAAT DER NEDERLANDEN (MINISTERIE VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES)**,  
gedaagde,  
gevestigd te Den Haag,  
advocaat mr. E.J. Daalder te Den Haag.

---

Eisers zullen hierna ieder afzonderlijk worden aangeduid zoals in de kop van dit vonnis vermeld en gezamenlijk als eisers. Gedaagde zal worden aangeduid als de Staat.

## **1. De procedure**

1.1. Het verloop van de procedure blijkt uit:

- de dagvaarding van 6 november 2013,
- de akte houdende wijziging van eis aan de zijde van eisers,
- de conclusie van antwoord, met twintig producties,
- het vonnis van 26 februari 2014, waarbij tevens een comparitie van partijen is gelast,
- het proces-verbaal van comparitie van 13 mei 2014 en de daarin genoemde akte houdende overlegging producties aan de zijde van eisers, met 44 producties, en de brief van 28 april 2014 van mr. Daalder, met twee producties,
- de brief van mr. Daalder van 30 mei 2014 naar aanleiding van het proces-verbaal van comparitie.

1.2. Ten slotte is vonnis bepaald op heden.

## **2. De feiten**

### *Procespartijen*

2.1. Nooitgedagt is strafrechtadvocaat. Tot zijn cliënten behoren uit de aard van zijn praktijk verdachten van strafbare feiten. Hij staat bovendien geregeld verdachten van (internationaal) terrorisme bij. Nooitgedagt rekent onder anderen Amerikaanse verdachten tot zijn cliënten. Hij behandelt ook uitleveringszaken, onder meer van verdachten van Nederland naar de Verenigde Staten van Amerika (hierna: VS).

2.2. De Winter is onderzoeksjournalist. Hij is in 2011 verkozen tot journalist van het jaar. Hij publiceert over databeveiliging en -veiligheid, met name bij de overheid. Hij behandelt overwegend politiek gevoelige onderwerpen. Zijn bronnen bestaan onder anderen uit personen die zwakheden in databeveiliging blootleggen. Hij communiceert met deze en andere personen via e-mail en telefoon.

2.3. Van Beek is adviseur informatiebeveiliging, verbonden aan Dexlab. Van Beek wordt door zijn cliënten gevraagd om in te breken op hun systemen om de beveiliging van gevoelige systemen te controleren. Daarnaast voert Van Beek onderzoek uit op het gebied van dataveiligheid en -beveiliging. De doelsystemen zijn vaak eigendom van Amerikaanse bedrijven en bevinden zich dikwijls op Amerikaans grondgebied. Van Beek bezoekt geregeld de VS.

2.4. Gonggrijp is een Nederlandse hacker die zich inzet voor transparantie van overheden. Hij is onder meer betrokken geweest bij de initiatieven van de organisatie van Wiki Leaks om vertrouwelijke documenten van de Amerikaanse overheid te publiceren. Hij is in dat kader onderwerp van onderzoek van Amerikaanse opsporingsautoriteiten. Bij het sociale communicatienetwerk Twitter zijn door hem gebruikte IP-adressen opgevraagd. Gonggrijp belt en mailt regelmatig met personen in de VS.

2.5. Paapst is werkzaam als onderzoeker en als docent bij de rechtenfaculteit van de Rijksuniversiteit Groningen. Hij is onder meer gespecialiseerd in de toepassing van het recht

op IT-systemen. In zijn onderzoek richt hij zich op 'internetgovernance', de wijze waarop internet wordt gereguleerd. In dat kader zijn de macht van de Amerikaanse regering en de bescherming van mensenrechten op het internet onderwerp van discussie. Paapst heeft zich in zijn publicaties kritisch uitgelaten over de Amerikanen en communiceert hierover geregeld vertrouwelijk via de e-mail met andere wetenschappers in binnen- en buitenland.

2.6. De NVSA is een vereniging die zich blijkens haar statuten onder meer ten doel stelt *"(...) al datgene, dat voor een goed functioneren van een verdediging in strafzaken dienstig is en zonodig daartoe in rechte op te treden."* Bijna alle in Nederland gespecialiseerde strafrechtadvocaten zijn lid van de NVSA.

2.7. De NVJ is een vereniging die zich blijkens haar statuten onder meer ten doel stelt *"nationaal en internationaal te waken en waar nodig te strijden voor de persvrijheid en het recht op informatie van de burgers, welke vrijheid en welk recht zij beschouwt als haar wezenlijke grondslagen"*, welk doel zij tracht te realiseren via alle wettige middelen en onder meer in het bijzonder door het *"vertegenwoordigend, regelend of bemiddelend optreden bij gelegenheden en gebeurtenissen waar een journalistiek, sociaal-economisch of algemeen maatschappelijk belang betrokken is, alsmede het verlenen van faciliteiten in verband met beroepsbezigheden."*

2.8. Internet Society Nederland is een vereniging die zich blijkens haar statuten onder meer ten doel stelt *"het stimuleren van gebruik en toepassingen van het Internet in Nederland en het participeren in de evolutie en ontwikkelingen van het Internet in een internationale context"*, welk doel zij tracht te realiseren onder meer door *"het verrichten van al hetgeen met het vorenstaande, waaronder begrepen het behartigen van de belangen van leden, in de ruimste zin genomen, in verband staat of daartoe bevorderlijk kan zijn."*

2.9. Privacy First is een stichting die zich blijkens haar statuten ten doel stelt *"het behouden en bevorderen van het recht op privacy, alsmede de persoonlijke vrijheid van leefomgeving, op welke wijze dan ook, onder meer door het in rechte optreden voor alle burgers in Nederland ter bescherming van dit algemene belang en voorts al hetgeen met een en ander rechtstreeks of zijdelings verband houdt of daartoe bevorderlijk kan zijn, alles in de ruimste zin van het woord."*

*De 'Snowden-onthullingen', mediapublicaties daarna en reacties bewindslieden en kabinet*

2.10. Op 6 juni 2013 werd door publicaties in de Britse krant *The Guardian* en de Amerikaanse krant de *Washington Post* bekend dat Edward Snowden, een voormalige contractant van de Amerikaanse National Security Agency (hierna: de NSA), geclassificeerde documenten van de NSA beschikbaar heeft gesteld aan de pers. Deze documenten hebben hoofdzakelijk betrekking op de activiteiten van de NSA en in beperkte mate op activiteiten van inlichtingendiensten van andere landen, zoals de Britse inlichtingendienst *Government Communications Headquarters* (hierna: de GCHQ). In deze eerste publicaties is met name het gebruik van het programma 'PRISM' door de NSA beschreven, een computerprogramma voor de vergaring van informatie van aanbieders van elektronische communicatie voor inlichtingendoelinden.

2.11. Later is in perspublicaties beschreven dat de GCHQ gebruikmaakt van een met 'PRISM' vergelijkbaar programma, 'TEMPORA' genoemd, en is melding gemaakt van allerlei andere surveillanceprogramma's waarvan de NSA en de GCHQ volgens de

---

publicaties gebruik maken bij de vergaring van informatie voor inlichtingen- en veiligheidsdoeleinden.

2.12. Bij brief van 21 juni 2013 aan de Tweede Kamer (*Kamerstukken II 2012/2013*, 30 977, nr. 56) heeft de minister van Binnenlandse Zaken en Koninkrijksrelaties (hierna: Binnenlandse Zaken) namens het kabinet uiteengezet hoe de wettelijke bevoegdheden van de Nederlandse inlichtingen- en veiligheidsdiensten zich verhouden tot 'PRISM'. Als bijlage is een factsheet van de Amerikaanse Director of National Intelligence van 8 juni 2013, getiteld "*Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*" met een toelichting op het programma 'PRISM' ter inzage gelegd. Blijkens de factsheet is 'PRISM': "*an internal government computer system used to facilitate the government's statutorily authorized collection of foreign intelligence information from electronic communication service providers under court supervision, as authorized by Section 702 of the Foreign Intelligence Surveillance Act (FISA) (50 U.S.C. § 1881a). This authority was created by the Congress and has been widely known and publicly discussed since its inception in 2008.*" In de brief van de minister van Binnenlandse Zaken is onder meer vermeld: "*De AIVD en de MIVD gebruiken het computerprogramma PRISM niet. De AIVD en de MIVD hebben geen onbelemmerde, onbeperkte toegang tot het internetverkeer en het mobiele telefoonverkeer, ook niet via buitenlandse inlichtingen- en veiligheidsdiensten. In het kader van de samenwerking met diensten in andere landen kunnen de AIVD en de MIVD wel gegevens uitwisselen. Artikel 59 van de Wiv 2002 [toevoeging rechtbank: Wet op de inlichtingen en veiligheidsdiensten 2002, hierna: Wiv 2002] beschrijft de kaders hiervoor. De mate van samenwerking met een buitenlandse dienst wordt onder meer bepaald door de democratische inbedding van de dienst en het respect voor de mensenrechten in het desbetreffende land, de betrouwbaarheid en de professionaliteit van de betrokken dienst en het operationele belang van de samenwerking. Het is de AIVD en de MIVD niet toegestaan diensten in andere landen verzoeken te doen die op grond van de Wiv 2002 niet zijn toegestaan. Het is overigens niet gebruikelijk dat diensten elkaar op de hoogte stellen van de eigen bronnen en de modus operandi. De wijze waarop specifieke gegevens zijn verkregen, wordt doorgaans niet gedeeld.*"

2.13. Bij brief van 3 juli 2013 aan de Tweede Kamer (*Kamerstukken II 2012/2013*, 30 977, nr. 59) heeft de minister van Binnenlandse Zaken gereageerd op het artikel op de website Nu.nl over een artikel dat op de website van de Britse krant *The Guardian* heeft gestaan en na korte tijd is ingetrokken en de Tweede Kamer geïnformeerd welke activiteiten van de Amerikaanse NSA bij de regering bekend waren. Daarin is onder meer vermeld: "*De mate van samenwerking met een buitenlandse dienst wordt onder meer bepaald op basis van de democratische inbedding van de collega-dienst, het respect voor de mensenrechten van het desbetreffende land, de betrouwbaarheid en de professionaliteit van de dienst en het operationele belang van de samenwerking. De internationale samenwerking wordt in bepaalde gevallen vastgelegd in Memoranda of Understanding (MoU's), die de basis vormen voor de wijze van informatie-uitwisseling met partnerdiensten. Over de vorm van samenwerking met specifieke buitenlandse diensten worden in het openbaar geen mededelingen gedaan. Internationale samenwerking is noodzakelijk voor de taakuitvoering van de diensten en vindt plaats binnen het kader van de Wet op de inlichtingen- en veiligheidsdiensten 2002 (Wiv 2002). De Nederlandse regering was voorafgaand aan de desbetreffende mediaberichten niet op de hoogte van de vermeende Amerikaanse spionageactiviteiten jegens EU-diplomaten. Zij is wel bekend met de Amerikaanse wetgeving op het gebied van buitenlandse inlichtingenvergaring. Het betreft onder meer sectie 702 van de Foreign Intelligence Surveillance Act. De factsheet van de Amerikaanse Director of National Intelligence van 8 juni 2013 heeft hiernaar verwezen. Deze is als bijlage bij de brief over het Amerikaanse programma PRISM van 21 juni jl. aan de Kamer gezonden (Kamerstuk 30 977, nr. 56).*"

---

*Inmiddels is besloten een EU-VS-expertgroep in te stellen om deze onderwerpen nader te bespreken. De AIVD en de MIVD zijn niet bevoegd verzoeken te doen aan buitenlandse collega-diensten om activiteiten uit te voeren die de Wiv 2002 de Nederlandse diensten niet toestaat. Dat geldt ook voor ongerichte interceptie van de kabelinfrastructuur. Het is niet gebruikelijk dat diensten elkaar op de hoogte stellen van de eigen bronnen en de modus operandi. De wijze waarop specifieke gegevens zijn verkregen, wordt doorgaans niet gedeeld. Voor zover in het kader van de internationale samenwerking collega-diensten hun werkwijzen bij de AIVD of de MIVD bekend hebben gemaakt, worden hierover in het openbaar geen mededelingen gedaan."*

2.14. In een Algemeen Overleg van de vaste commissie voor Defensie van 3 juli 2013 (*Kamerstukken II 2012/2013*, 29 924, nr. 100) heeft de minister van Defensie over 'PRISM' onder meer opgemerkt: "Voor mij is het van belang om te weten of wij op de hoogte waren. Had ik op de hoogte kunnen zijn van het programma PRISM? Het antwoord op die vraag is «nee». Kan ik uitsluiten dat er ooit wordt gebruikgemaakt van gegevens die via het programma PRISM bij onze diensten zijn beland? Het antwoord op die vraag is ook «nee»."

2.15. Op 4 juli 2013 heeft de Tweede Kamer besloten (*Kamerstukken II 2012/2013*, 30 977, nr. 57) de commissie van toezicht betreffende de inlichtingen- en veiligheidsdiensten (CTIVD) te verzoeken onderzoek te verrichten naar de dataverzameling door de Algemene Inlichtingen- en Veiligheidsdienst (hierna: AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (hierna: MIVD), welk verzoek op 16 juli 2013 is gedaan.

2.16. Bij brief van 13 september 2013 van de minister van Binnenlandse Zaken, mede namens de ministers van Defensie, van Buitenlandse Zaken en van Veiligheid en Justitie aan de Tweede Kamer (*Kamerstukken II 2013/2014*, 30 977, nr. 61) is kabinetsbreed onder meer als volgt gereageerd op de onthullingen van de heer Snowden: "Het kabinet volgt met aandacht de reactie van de Verenigde Staten op de onthullingen van de heer Snowden. Het kabinet hecht, zoals eerder gemeld, zeer aan zorgvuldige en deugdelijke bescherming van persoonsgegevens. Het is daarom noodzaak om waar nationale veiligheid en privacybescherming elkaar raken, zo transparant mogelijk te zijn over procedures, bevoegdheden, waarborgen en toezichtmaatregelen. Het kabinet acht het in dat verband bemoedigend dat Amerikaanse Congresleden juist over die onderwerpen debatteren en voorstellen doen voor wijziging van de regelgeving en dat ook president Obama in zijn persconferentie van 9 augustus jl. heeft verklaard meer transparantie en toezicht na te streven. Het is tevens verheugend dat de Amerikaanse regering hiermee inmiddels een begin heeft gemaakt door meer inzicht te geven in de bevoegdheden en door publicatie van de juridische onderbouwing van enkele programma's. Nederland is hierover in gesprek met de Verenigde Staten."

2.17. Op 21 oktober 2013 is op de website 'Tweakers.net' een bericht verschenen over het afluisteren van Nederlanders door de NSA. Het bericht is gebaseerd op een artikel in de Franse krant *Le Monde* van diezelfde dag. Het artikel in *Le Monde* geeft een nadere duiding aan een grafiek die op 5 augustus 2013 door het Duitse weekblad *Der Spiegel* is gepubliceerd.

2.18. Bij brief van 28 oktober 2013 aan de Tweede Kamer (*Kamerstukken II 2013/2014*, 30 977, nr. 63) heeft de minister van Binnenlandse Zaken, mede namens de ministers van Veiligheid en Justitie, van Buitenlandse Zaken en van Defensie op deze mediaberichten gereageerd. In deze brief is onder meer vermeld:

*"Uit de mediaberichten zou blijken dat de Amerikaanse diensten de metadata van telefoonverkeer opslaan voor nadere analyse. Het betreft bijvoorbeeld gegevens over wie er belt, wanneer en hoe*

lang, en vanuit welk gebied. Na die nadere analyse zou de NSA er voor kunnen kiezen de inhoud van de communicatie te bekijken in overeenstemming met de daarvoor geldende eisen volgens Amerikaanse wetgeving. Gezien de Amerikaanse wetgeving, waaronder de Foreign Intelligence Surveillance Act (FISA), is het kabinet zich bewust van de mogelijkheid dat de Amerikaanse NSA telefooncommunicatie kan onderscheppen. Met behulp van de analyse van metadata kunnen netwerken van personen en organisaties in kaart worden gebracht, en kan de intensiteit van de contacten worden ingeschat.

*Standpunt Nederlandse kabinet*

Het kabinet acht op zichzelf het intercepteren van metadata en het analyseren daarvan in zijn algemeenheid een aanvaardbare methode in het kader van onderzoek naar terroristen, andere gevaren voor de nationale veiligheid of in het kader van militaire operaties (zie art. 26 en 27 van de Wet op de Inlichtingen- en Veiligheidsdiensten). Het af luisteren van telefoonverkeer en het aftappen van emailverkeer in Nederland door inlichtingen- en veiligheidsdiensten kan alleen geschieden binnen de kaders van de Wet op de Inlichtingen- en veiligheidsdiensten 2002 en alleen op last van de desbetreffende ministers. Iedere andere vorm is niet acceptabel. Het kan voorkomen dat andere landen menen dat er een goede reden is om in of vanuit Nederland inlichtingen te verzamelen. In een dergelijk geval dient het desbetreffende land een verzoek te richten tot de AIVD of de MIVD. Het verzoek wordt dan binnen de kaders van de Nederlandse wet beoordeeld. Het kabinet acht enig optreden buiten die wettelijke kaders niet aanvaardbaar. De AIVD en de MIVD doen om die reden structureel onderzoek naar spionage van buitenlandse mogendheden in Nederland. Indien dergelijke spionage wordt geconstateerd, dan volgen altijd maatregelen. Dat geldt ook als bondgenoten ongewenste spionage-activiteiten in Nederland uitvoeren. In Nederland geldt de Nederlandse wet, ook voor bondgenoten."

2.19. Bij brief van 31 oktober 2013 aan de Tweede Kamer (*Kamerstukken II* 2013/2014, 30 977, nr. 64) heeft de minister van Binnenlandse Zaken schriftelijk gereageerd op twee moties die verband houden met de NSA. Blijkens deze brief betreffen de 1,8 miljoen telefoongesprekken die volgens de overwegingen van de moties zouden zijn afgeluisterd, respectievelijk onderschept, zogenoemde metadata. Metadata (hierna ook: metagegevens) zijn gegevens over communicatie. In het geval van bijvoorbeeld een telefoongesprek gaat het hier om de betrokken telefoonnummers, de begintijd en de eindtijd van het gesprek en de gegevens van de betrokken zendmasten. In de brief is een verklaring van de NSA in reactie op de perspublicaties opgenomen:

*"Statement on articles in European press alleging large numbers of phone call metadata collected by NSA in France, Spain, Italy*

*The assertions by reporters in France (Le Monde), Spain (El Mundo) and Italy (L'Espresso) that NSA collected 10s of millions of phone calls are completely false. They cite as evidence screen shots of the results of a web tool used for data management purposes, but both they and the person who stole the classified data did not understand what they were looking at. The web tool counts metadata records from around the world and displays the totals in several different formats. The sources of metadata include data legally collected by NSA under its various authorities, as well as metadata provided to NSA by foreign partners. To be perfectly clear, this is not information that we collected on European citizens. It represents information that we and our NATO allies have collected in defense of our countries and in support of military operations."*

2.20. Bij brief van 5 november 2013 aan de Tweede Kamer (*Kamerstukken II* 2013/2014, 30 977, nr. 65) heeft de minister van Binnenlandse Zaken gereageerd op een artikel in de *Volkskrant* van 4 november 2013 over de werkwijze van de NSA, waarin onder meer vermeld is dat de Nederlandse inlichtingen- en veiligheidsdiensten deel zouden uitmaken van het zogenaamde 'Nine Eyes'-samenwerkingsverband. In de brief is onder meer vermeld:

*"De AIVD en de MIVD werken uiteraard samen met andere I&V-diensten. Dat is van groot belang*

voor onze eigen nationale veiligheid. Die samenwerking vindt plaats binnen de kaders van de wet. De Commissie van toezicht betreffende de Inlichtingen- en Veiligheidsdiensten (CTIVD) houdt toezicht op de activiteiten van de AIVD en de MIVD.

De Nederlandse diensten hebben een duidelijk wettelijk kader waarbinnen zij werken en zorgdragen voor de veiligheid van Nederland. In de Wet op de Inlichtingen- en Veiligheidsdiensten 2002 (Wiv 2002) is een zorgvuldige afweging gemaakt tussen privacy en veiligheid. De AIVD en de MIVD mogen geen verzoeken doen aan buitenlandse I&V-diensten die op grond van de Nederlandse wet niet zijn toegestaan. Ook hier houdt de CTIVD toezicht op.

Er kunnen in het openbaar geen mededelingen worden gedaan over specifieke samenwerkingsrelaties of operaties van de AIVD en de MIVD." Op vragen naar de genoemde 'Nine Eyes' heeft de minister van Binnenlandse Zaken tijdens een overleg met de vaste commissie voor Binnenlandse Zaken op 6 november 2013 (*Kamerstukken II 2013/2014*, 30 977, nr. 75) meegedeeld dat hij over de samenwerking met de VS slechts kan zeggen dat als bondgenoten wordt samengewerkt.

2.21. Naar aanleiding van een bericht in *NRC Handelsblad* van 23 november 2013 dat Nederland in het verleden doelwit is geweest van de NSA heeft de minister van Binnenlandse Zaken bij brief van 27 november 2013 aan de Tweede Kamer (*Kamerstukken II 2013/2014*, 30 977, nr. 74) bericht dat hij dat niet kan bevestigen en dat het Ministerie contact opneemt met de Amerikaanse ambassade om te vragen of zij de berichtgeving kan bevestigen. Verder is in deze brief vermeld: "Inlichtingen- en veiligheidsdiensten maken niet bekend in welke landen zij onderzoek doen. De NSA heeft eerder gemeld dat Nederland geen doelwit is. Deze mededeling betreft het heden. De berichten in het *NRC Handelsblad* hebben daarop geen betrekking. Het kan voorkomen dat andere landen menen dat er een goede reden is om in of vanuit Nederland inlichtingen te verzamelen. In een dergelijk geval dient het desbetreffende land een verzoek te richten tot de AIVD of de MIVD. Het verzoek wordt dan binnen de kaders van de Nederlandse wet beoordeeld en eventueel uitgevoerd. Het kabinet acht enig optreden buiten die wettelijke kaders niet aanvaardbaar."

*Rapporten Commissie evaluatie Wiv 2002 en CTIVD, reacties kabinet, kamerdebat van 9 april 2014*

2.22. Op 2 december 2013 heeft de Commissie evaluatie Wiv 2002 haar rapport "Evaluatie van de Wet op de inlichtingen- en veiligheidsdiensten 2002, Naar een nieuwe balans tussen bevoegdheden en waarborgen" aan het kabinet uitgebracht en is dit rapport aan de Tweede Kamer aangeboden (*Kamerstukken II 2013/2014*, 33 820, nr. 1). De Commissie evaluatie Wiv 2002 is tot de bevinding gekomen dat de Wiv 2002 aanpassing behoeft. Die conclusie is blijkens het rapport: "vooral ingegeven door de onstuitbare en vergaande technologische ontwikkelingen omdat die zowel de aandachtsgebieden en mogelijkheden van de I&V-diensten verruimen, en dat ook moeten doen, als dat ze de mogelijke inbreuken op de grondrechten van burgers kunnen vergroten. De voortdurende stroom aan publicaties over internet- en telefoonintercepties (PRISM) gedurende een groot deel van de onderzoeksperiode van de evaluatiecommissie heeft de potentieel vergaande gevolgen van de technologische ontwikkelingen nog eens onderstreept. Tegen deze achtergrond heeft de evaluatiecommissie de aanbevelingen over de aanpassingen in de Wiv 2002 ontwikkeld." Op het punt van samenwerking tussen de diensten en andere organisaties concludeert Commissie evaluatie Wiv 2002 als volgt: "De evaluatiecommissie vindt dat de bepalingen in de Wiv over de samenwerking van de diensten met andere instanties op onderdelen aanpassing behoeven. Artikel 59 over de samenwerking van beide diensten met buitenlandse zusterorganisaties verdient heroverweging. Mede in het licht van de recente discussies over de activiteiten van de NSA, moet nader onderzocht worden of de Wiv voor de samenwerking met buitenlandse diensten voldoende rechtsstatelijke en democratische garanties bevat."

2.23. Bij brief van 11 maart 2014 heeft het kabinet gereageerd op dit rapport (*Kamerstukken II* 2013/2014, 33 820, nr. 2). De reactie bevat onder meer de volgende passage: *“Het recht op bescherming van de persoonlijke levenssfeer is evenwel niet absoluut, maar kan onder bepaalde omstandigheden worden beperkt. Voor de activiteiten van de Nederlandse inlichtingen- en veiligheidsdiensten biedt de Wiv 2002 deze wettelijke grondslag. In deze wet is limitatief vastgelegd op welke wijze de diensten door gebruikmaking van de aan hen toegekende bevoegdheden op het recht op privacy een inbreuk mogen maken. In alle gevallen moet daarbij worden voldaan aan de eisen van noodzakelijkheid, proportionaliteit en subsidiariteit. Deze bevoegdheidsuitoefening is bovendien uitsluitend toegestaan indien het belang van de nationale veiligheid, zoals dat nader is uitgewerkt in de taakstelling van de diensten (artikel 6 en 7), daartoe noodzaakt.*

*Het kabinet merkt het volgende op. In zijn algemeenheid wordt aangenomen dat waar het gaat om telecommunicatie, dat hoe dichter bij de inhoud van die communicatie (de ‘content’) wordt gekomen ook de inbreuk groter wordt. Naar het oordeel van het kabinet is het hieraan ten grondslag liggende onderscheid tussen inhoud (content) en niet-inhoud (metadata) niet het enige bepalende element bij het vaststellen van de ernst van de inbreuk en bij het daarop toe te snijden model van toestemming, zoals dat in een mogelijk voor te bereiden wetsvoorstel zal worden neergelegd. Evenzeer is van belang de schaal waarop gegevens worden verzameld en hoe ingrijpend de gehanteerde ontsluitingsmethodiek is voor de privacy van de burger. Bulk interceptie en de toepassing van verfijnde methodieken van metadata-analyse kunnen onder omstandigheden ingrijpender zijn dan een kortstondige interceptie van de inhoud van de telecommunicatie.”* Naar aanleiding van de aanbeveling betreffende de samenwerking tussen diensten en andere organisaties merkt het kabinet het volgende op: *“Artikel 59 verdient volgens de Commissie heroverweging. Nader onderzocht zou moeten worden of de wet voldoende rechtsstatelijke en democratische garanties biedt bij de samenwerking met buitenlandse diensten. Waarborgen bij of criteria voor samenwerking zijn niet opgenomen in de wet. Het kabinet merkt op dat wereldwijde internationale samenwerking voor de inlichtingen- en veiligheidsdiensten een conditio sine qua non is. De aard en intensiteit van die samenwerking moet mede worden bepaald door criteria als de democratische inbedding van de desbetreffende dienst, het mensenrechtenbeleid van het desbetreffende land, de professionaliteit en betrouwbaarheid en het karakter van de dienst. Het kabinet onderschrijft dat de wet daarvoor voldoende kader en ruimte moet bieden. De uitwisseling van bulkdata met buitenlandse diensten zal bovendien worden onderworpen aan een systeem van ministeriële toestemming.”*

2.24. Eveneens op 11 maart 2014 hebben de ministers van Binnenlandse Zaken en van Defensie het Toezichtsrapport van de CTIVD inzake gegevensverwerking op het gebied van telecommunicatie door de AIVD en MIVD van 5 februari 2014 (rapport nr. 38) aangeboden aan de Tweede Kamer (*Kamerstukken II* 2013/2014, 29 924, nr. 105). In dit rapport staan, in lijn met het verzoek van de Tweede Kamer, de volgende vier onderwerpen centraal:

1. de reikwijdte van de algemene en bijzondere bevoegdheden van de diensten tot gegevensverwerking op het gebied van telecommunicatie, mede in relatie tot de Grondwet en het EVRM;
2. de wijze waarop gebruik gemaakt wordt van verschillende soorten gegevensbestanden door de diensten en de regels die gelden voor dat gebruik;
3. de mogelijkheden en beperkingen van de uitwisseling van gegevens met buitenlandse inlichtingen- en/of veiligheidsdiensten;
4. de wijze waarop de door het EVRM gestelde toetsingsnormen – noodzakelijkheid, proportionaliteit en subsidiariteit – een rol spelen bij de gegevensverwerking door de diensten, in het bijzonder bij de gegevensuitwisseling met buitenlandse inlichtingen- en/of veiligheidsdiensten.



2.25. Eerdere rapporten van de CTIVD, voor zover van belang op dit terrein, zijn het Toezichtsrapport inzake de samenwerking van de AIVD met buitenlandse inlichtingen- en/of veiligheidsdiensten van 12 augustus 2009 (rapport nr. 22A), het Toezichtsrapport inzake de inzet van sigint door de MIVD van 23 augustus 2011 (rapport nr. 28) en het Toezichtsrapport inzake de inzet van de af luisterbevoegdheid tot de selectie van sigint door de AIVD van 11 april 2012 (rapport nr. 31). ‘Sigint’ is de afkorting van “Signal intelligence” en staat voor inlichtingen die verzameld worden uit opgevangen elektronische signalen.

2.26. In haar rapport van 5 februari 2014 schetst de CTIVD op basis van haar onderzoek het volgende beeld: *“De AIVD en de MIVD zijn de afgelopen jaren in toenemende mate gaan werken met verzamelingen (persoons)gegevens. Dit hangt samen met nieuwe technische mogelijkheden en de digitalisering van de samenleving. De Commissie signaleert dat beide diensten zowel bij het verwerven van gegevens als bij de uitwisseling met buitenlandse diensten de bepalingen in de Wiv 2002 als uitgangspunt nemen. Bestaande bevoegdheden worden echter op manieren ingezet die bij de totstandkoming van de wet niet altijd waren voorzien. Naar het oordeel van de Commissie bieden sommige werkwijzen van de diensten op bepaalde vlakken thans onvoldoende waarborgen voor de bescherming van de persoonlijke levenssfeer. In enkele gevallen zijn deze werkwijzen onrechtmatig op basis van de Wiv 2002, bijvoorbeeld vanwege het ontbreken van motivering en/of toestemming op het juiste niveau. De Commissie constateert dat de AIVD en de MIVD in enkele hechte samenwerkingsverbanden verzamelingen (ruwe) gegevens uitwisselen. Hierbij wordt erop vertrouwd dat buitenlandse diensten mensenrechten respecteren en handelen binnen hun eigen wettelijk kader. De Commissie is van mening dat het in het licht van de onthullingen van de afgelopen periode gewenst is om na te gaan of dit vertrouwen nog steeds terecht is. Zij beveelt de betrokken ministers in dit verband tevens aan de samenwerkingsrelaties (ook in internationaal verband) te beoordelen op transparantie en de afwegingen die ten grondslag liggen aan de samenwerking nader te concretiseren.”*

2.27. In de aanbiedingsbrief van 11 maart 2014 bij dit rapport hebben de ministers van Binnenlandse Zaken en van Defensie aan de Tweede Kamer meegedeeld dat de aanbevelingen van de CTIVD in haar rapport van 5 februari 2014 worden opgevolgd.

2.28. Op 9 april 2014 heeft een debat plaatsgevonden over het af luisteren door de NSA en de rol van Nederland daarin (*Handelingen II* 2013/2014, nr. 73). Tijdens dit debat heeft de minister van Binnenlandse Zaken onder meer (opnieuw) meegedeeld dat in de wet zal worden vastgelegd dat voor het samenwerken met andere diensten de criteria mensenrechten, democratische inbedding, professionaliteit en betrouwbaarheid belangrijke wegingsfactoren zijn. Over de zogenoemde U-bocht-constructie heeft hij meegedeeld: *“De U-bochtconstructie - de terminologie is hier gelanceerd - betreft het systematisch vragen aan een bondgenoot om dingen voor ons te doen die we zelf niet mogen doen. De dienst heeft dat niet geconstateerd. Nogmaals, hiermee kan niet uitgesloten worden dat als wij op een specifiek risico worden gewezen, de informatie daarover verkregen is in een lange keten waarin misschien ook een keer iets is gedaan wat niet had gemogen volgens de Nederlandse wet. Dat kan ik niet uitsluiten. Dat vind ik echter geen U-bocht meer.”*

*Enige reacties op de Snowden-onthullingen in Europees verband*

2.29. Eind juli 2013 heeft de Europese Commissie een ad hoc EU-VS-expertgroep ingesteld met als doel: *“to establish the facts about US surveillance programmes and their impact on fundamental rights in the EU and personal data of EU citizens.”*

2.30. De EU-VS-expertgroep heeft op 27 november 2013 gerapporteerd. Met betrekking tot de verzameling en verdere verwerking van gegevens is in het rapport (hoofdstuk 3) onder meer vermeld: *"In response to questions from the EU regarding how data is collected and used under the surveillance programmes, the US stated that the collection of personal information based on Section 702 FISA and Section 215 Patriot Act is subject to a number of procedural safeguards and limitative conditions. Under both legal authorities, according to the US, privacy is protected by a multi-layered system of controls on what is collected and on the use of what is collected, and these controls are based on the nature and intrusiveness of the collection. It appeared from the discussions that there is a significant difference in interpretation between the EU and the US of a fundamental concept relating to the processing of personal data by security agencies. For the EU, data acquisition is synonymous with data collection and is a form of processing personal data. Data protection rights and obligations are already applicable at that stage. Any subsequent operation carried out on the data collected such as storage or consultation by human eyes, constitutes further processing. As the US explained, under US law, the initial acquisition of personal data does not always constitute processing of personal data.; data is "processed" only when it is analysed by means of human intervention. This means that while certain safeguards arise at the moment of acquisition, additional data protection safeguards arise at the time of processing."*

2.31. De samenvatting van de hoofdconclusies van dit rapport van de EU-VS-expertgroep luidt als volgt:

*"(1) Under US law, a number of legal bases allow large-scale collection and processing, for foreign intelligence purposes, including counter-terrorism, of personal data that has been transferred to the US or is processed by US companies. The US has confirmed the existence and the main elements of certain aspects of these programmes, under which data collection and processing is done with a basis in US law that lays down specific conditions and safeguards. Other elements remain unclear, including the number of EU citizens affected by these surveillance programmes and the geographical scope of surveillance programmes under Section 702.*

*(2) There are differences in the safeguards applicable to EU data subjects compared to US data subjects, namely:*

*i. Collection of data pertaining to US persons is, in principle, not authorised under Section 702.*

*Where it is authorised, data of US persons is considered to be "foreign intelligence" only if necessary to the specified purpose. This necessity requirement does not apply to data of EU citizens which is considered to be "foreign intelligence" if it relates to the purposes pursued. This results in lower threshold being applied for the collection of personal data of EU citizens.*

*ii. The targeting and minimisation procedures approved by FISC under Section 702 are aimed at reducing the collection, retention and dissemination of personal data of or concerning US persons. These procedures do not impose specific requirements or restrictions with regard to the collection, processing or retention of personal data of individuals in the EU, even when they have no connection with terrorism, crime or any other unlawful or dangerous activity. Oversight of the surveillance programmes aims primarily at protecting US persons.*

*iii. Under both Section 215 and Section 702, US persons benefit from constitutional protections (respectively, First and Fourth Amendments) that do not apply to EU citizens not residing in the US.*

*(3) Moreover, under US surveillance programmes, different levels of data protection safeguards apply to different types of data (meta-data vs. content data) and different stages of data processing (initial acquisition vs. further processing/analysis).*

*(4) A lack of clarity remains as to the use of other available legal bases, the existence of other surveillance programmes as well as limitative conditions applicable to these programmes. This is especially relevant regarding Executive Order 12333.*

*(5) Since the orders of the FISC are classified and companies are required to maintain secrecy*

*with regard to the assistance they are required to provide, there are no avenues, judicial or administrative, for either EU or US data subjects to be informed of whether their personal data is being collected or further processed. There are no opportunities for individuals to obtain access, rectification or erasure of data, or administrative or judicial redress.*

*(6) Various layers of oversight by the three branches of Government apply to activities on the base of Section 215 and Section 702. There is judicial oversight for activities that imply a capacity to compel information, including FISC orders for the collection under Section 215 and annual certifications that provide the basis for collection under Section 702. There is no judicial approval of individual selectors to query the data collected under Section 215 or tasked for collection under Section 702. The FISC operates ex parte and in camera. Its orders and opinions are classified, unless they are declassified. There is no judicial oversight of the collection of foreign intelligence outside the US under Executive Order 12333, which are conducted under the sole competence of the Executive Branch."*

2.32. De Committee on Civil Liberties, Justice and Home Affairs van het Europees Parlement heeft bij monde van Claude Moraes op 21 februari 2014 gerapporteerd aan het Europees Parlement, met onder meer de volgende aanbeveling: "26. *Calls on the Member States, including when represented by their intelligence agencies, to refrain from accepting data from third states which have been collected unlawfully and from allowing surveillance activities on their territory by third states' governments or agencies which are unlawfully under national law or do not meet the legal safeguards enshrined in international or EU-instruments, including the protection of human rights under the THEU, the ECHR and the EU Chapter of Fundamental Rights.*"

2.33. Op 10 april 2014 heeft de 'Article 29 Data Protection Working Party', een onafhankelijk Europees adviesorgaan "on data protection and privacy", opgericht op grond van Richtlijn 95/46/EC (Richtlijn van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, hierna: Dataprotectierichtlijn), een rapport uitgebracht, inhoudende een "Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes".

### **3. De Wiv 2002**

3.1. De werkzaamheden van de AIVD en de MIVD (hierna gezamenlijk ook: de diensten) zijn geregeld in de Wiv 2002. Zij hebben in het belang van de nationale veiligheid een aantal in de Wiv 2002 genoemde taken.

3.2. De AIVD heeft in het belang van de nationale veiligheid tot taak (artikel 6 lid 2 Wiv 2002):

*"a. het verrichten van onderzoek met betrekking tot organisaties en personen die door de doelen die zij nastreven, dan wel door hun activiteiten aanleiding geven tot het ernstige vermoeden dat zij een gevaar vormen voor het voortbestaan van de democratische rechtsorde, dan wel voor de veiligheid of voor andere gewichtige belangen van de staat;*

*b. het verrichten van veiligheidsonderzoeken als bedoeld in de Wet veiligheidsonderzoeken;*

*c. het bevorderen van maatregelen ter bescherming van de onder a genoemde belangen, waaronder begrepen maatregelen ter beveiliging van gegevens waarvan de geheimhouding door de nationale veiligheid wordt geboden en van die onderdelen van de overheidsdienst en van het bedrijfsleven die naar het oordeel van Onze ter zake verantwoordelijke Ministers van vitaal belang zijn voor de instandhouding van het maatschappelijk leven;*

*d. het verrichten van onderzoek betreffende andere landen ten aanzien van onderwerpen die door Onze Minister-President, Minister van Algemene Zaken, in overeenstemming met Onze betrokken Ministers zijn aangewezen;*

*e. het opstellen van dreigings- en risicoanalyses op verzoek van Onze Minister van Binnenlandse Zaken en Koninkrijksrelaties en Onze Minister van Veiligheid en Justitie gezamenlijk ten behoeve van de beveiliging van de personen, bedoeld in de artikelen 4, derde lid, onderdeel b, en 42, eerste lid, onder c, van de Politiewet 2012 en de bewaking en de beveiliging van de objecten en de diensten die zijn aangewezen op grond van artikel 16 van die wet.”*

3.3. De MIVD heeft in het belang van de nationale veiligheid tot taak (artikel 7 lid 2 Wiv 2002):

*“a. het verrichten van onderzoek:*

*1°. omtrent het potentieel en de strijdkrachten van andere mogendheden, ten behoeve van een juiste opbouw en een doeltreffend gebruik van de krijgsmacht;*

*2°. naar factoren die van invloed zijn of kunnen zijn op de handhaving en bevordering van de internationale rechtsorde voor zover de krijgsmacht daarbij is betrokken of naar verwachting betrokken kan worden;*

*b. het verrichten van veiligheidsonderzoeken als bedoeld in de Wet veiligheidsonderzoeken;*

*c. het verrichten van onderzoek dat nodig is voor het treffen van maatregelen:*

*1°. ter voorkoming van activiteiten die ten doel hebben de veiligheid of paraatheid van de krijgsmacht te schaden;*

*2°. ter bevordering van een juist verloop van mobilisatie en concentratie der strijdkrachten;*

*3°. ten behoeve van een ongestoorde voorbereiding en inzet van de krijgsmacht als bedoeld in onderdeel a, onder 2°.*

*d. het bevorderen van maatregelen ter bescherming van de onder c genoemde belangen, waaronder begrepen maatregelen ter beveiliging van gegevens betreffende de krijgsmacht waarvan de geheimhouding is geboden;*

*e. het verrichten van onderzoek betreffende andere landen, ten aanzien van onderwerpen met een militaire relevantie die door Onze Minister-President, Minister van Algemene Zaken, in overeenstemming met Onze betrokken Ministers, zijn aangewezen;*

*f. het opstellen van dreigingsanalyses op verzoek van Onze Minister van Binnenlandse Zaken en Koninkrijksrelaties en Onze Minister van Veiligheid en Justitie gezamenlijk ten behoeve van de beveiliging van de personen, bedoeld in de artikelen 4, derde lid, onderdeel b, en 42, eerste lid, onder c, van de Politiewet 2012 en de bewaking en de beveiliging van de objecten en de diensten die zijn aangewezen op grond van artikel 16 van die wet, voor zover het betreft personen, objecten en diensten met een militaire relevantie.”*

3.4. De Wiv 2002 bevat bepalingen met betrekking tot de verwerking van gegevens door de diensten. Gegevens in de zin van de Wiv 2002 zijn persoonsgegevens en andere gegevens (artikel 1 sub e Wiv 2002) en onder de verwerking van gegevens wordt verstaan (artikel 1 sub f Wiv 2002): *“elke handeling of geheel van handelingen met betrekking tot gegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.”* De diensten zijn bevoegd tot het verwerken van gegevens met inachtneming van de eisen die daaraan bij of krachtens de Wiv 2002 of de Wet veiligheidsonderzoeken zijn gesteld. Dit betekent onder meer dat de verwerking van gegevens slechts plaatsvindt voor een bepaald doel en slechts voor zover dat noodzakelijk is voor een goede uitvoering van deze wetten en dat de verwerking van gegevens slechts betrekking kan hebben op in de Wiv 2002, voor de AIVD en MIVD afzonderlijk genoemde, bepaalde personen (artikelen 12 en 13 Wiv 2002).

3.5. De diensten hebben op grond van de Wiv 2002 de algemene bevoegdheid om bij de uitvoering van hun taak, dan wel ter ondersteuning van een goede taakuitoefening, gegevens te verzamelen (artikel 17 Wiv 2002). Tevens zijn aan de diensten bijzondere bevoegdheden

toegekend (artikel 20-29 Wiv 2002). Deze bijzondere bevoegdheden mogen slechts worden uitgeoefend voor zover dat noodzakelijk is voor de goede uitvoering, wat betreft de AIVD, van de taken bedoeld in artikel 6 lid 2 sub a en d Wiv 2002 en, wat betreft de MIVD, van de taken bedoeld in artikel 7 lid 2 sub a, c en e Wiv 2002 (artikel 18 Wiv 2002). Voor de uitoefening van bijzondere bevoegdheden is, voor zover de wet niet anders bepaalt, toestemming van de betrokken minister of, namens deze, het hoofd van de desbetreffende dienst vereist. Op de uitoefening van de bijzondere bevoegdheden van de diensten zijn verder de beginselen van subsidiariteit en proportionaliteit van toepassing (uitgewerkt in de artikelen 31 en 32 Wiv 2002).

3.6. Bijzondere bevoegdheden van de diensten zijn onder meer het gericht ontvangen, opnemen en af luisteren van communicatie: *“De diensten zijn bevoegd tot het met een technisch hulpmiddel gericht aflappen, ontvangen, opnemen en af luisteren van elke vorm van gesprek, telecommunicatie of gegevensoverdracht door middel van een geautomatiseerd werk, ongeacht waar een en ander plaatsvindt. Tot de bevoegdheid, bedoeld in de eerste volzin, behoort tevens de bevoegdheid om versleuteling van de gesprekken, telecommunicatie of gegevensoverdracht ongedaan te maken”* (artikel 25 lid 1 Wiv 2002), het ontvangen en opnemen van niet-kabelgebonden communicatie dat zijn oorsprong of bestemming in andere landen heeft, aan de hand van een technisch kenmerk ter verkenning van de communicatie: *“De diensten zijn bevoegd tot het met een technisch hulpmiddel ontvangen en opnemen van niet-kabelgebonden telecommunicatie die zijn oorsprong of bestemming in andere landen heeft, aan de hand van een technisch kenmerk ter verkenning van de communicatie. De diensten zijn bevoegd om van daarbij ontvangen gegevens kennis te nemen. Tot de bevoegdheid, bedoeld in de eerste volzin, behoort tevens de bevoegdheid om versleuteling van de telecommunicatie ongedaan te maken”* (artikel 26 lid 1 Wiv 2002) en het ongericht ontvangen en opnemen van niet-kabelgebonden telecommunicatie en de selectie daarvan: *“De diensten zijn bevoegd tot het met een technisch hulpmiddel ongericht ontvangen en opnemen van niet-kabelgebonden telecommunicatie. Tot de bevoegdheid, bedoeld in de eerste volzin, behoort tevens de bevoegdheid om versleuteling van de telecommunicatie ongedaan te maken”* en *“De gegevens die door de uitoefening van de bevoegdheid, bedoeld in het eerste lid, zijn verzameld, kunnen door de diensten worden geselecteerd aan de hand van: a. gegevens betreffende de identiteit van een persoon dan wel een organisatie; b. een nummer als bedoeld in artikel 1.1, onder bb, van de Telecommunicatiewet, dan wel enig technisch kenmerk; c. aan een nader omschreven onderwerp gerelateerde trefwoorden”* (artikel 27 leden 1 en 3 Wiv 2002). Voor het ontvangen en opnemen van niet-kabelgebonden telecommunicatie ter verkenning van communicatie (ook ‘searchen’ genoemd) en voor het ongericht ontvangen en opnemen van niet-kabelgebonden telecommunicatie is geen toestemming van de betrokken minister vereist, voor de selectie van ongerichte kabelgebonden telecommunicatie wel (artikel 26 lid 2 en artikel 27 leden 2, 4 en 5 Wiv 2002). Het ongericht ontvangen en opnemen van kabelgebonden telecommunicatie is op grond van de Wiv 2002 niet toegestaan.

3.7. De samenwerking tussen de diensten en buitenlandse inlichtingen- en veiligheidsdiensten (hierna: buitenlandse diensten) is geregeld in artikel 59 Wiv 2002. Deze bepaling luidt als volgt:

1. De hoofden van de diensten dragen zorg voor het onderhouden van verbindingen met daarvoor in aanmerking komende inlichtingen- en veiligheidsdiensten van andere landen.
2. In het kader van het onderhouden van verbindingen als bedoeld in het eerste lid kunnen aan deze instanties gegevens worden verstrekt ten behoeve van door deze instanties te behartigen belangen, voor zover:
  - a. deze belangen niet onverenigbaar zijn met de belangen die de diensten hebben te behartigen, en

- 
- b. een goede taakuitvoering door de diensten zich niet tegen verstrekking verzet.*
- 3. Op de verstrekking van gegevens als bedoeld in het tweede lid, zijn de artikelen 37, 41 en 42 van overeenkomstige toepassing.*
- 4. In het kader van het onderhouden van verbindingen als bedoeld in het eerste lid kunnen voorts op een daartoe strekkend schriftelijk verzoek aan deze instanties technische en andere vormen van ondersteuning worden verleend ten behoeve van door deze instanties te behartigen belangen, voor zover:*
- a. deze belangen niet onverenigbaar zijn met de belangen die de diensten hebben te behartigen, en*
- b. een goede taakuitvoering door de diensten zich niet tegen de verlening van de desbetreffende vorm van ondersteuning verzet.*
- 5. Een verzoek om ondersteuning als bedoeld in het vierde lid dient ondertekend te zijn door de daartoe bevoegde autoriteit van deze instantie en omvat een nauwkeurige omschrijving van de verlangde vorm van ondersteuning alsmede de reden waarom de ondersteuning wenselijk wordt geacht. De verzochte ondersteuning wordt slechts verleend, indien daarvoor toestemming is verkregen van Onze betrokken Minister.*
- 6. Onze betrokken Minister kan de bevoegdheid tot het verlenen van toestemming als bedoeld in het vijfde lid uitsluitend mandateren aan het hoofd van de dienst, voor zover het gaat om verzoeken met een spoedeisend karakter. Van een verleende toestemming door het hoofd van de dienst wordt Onze betrokken Minister terstond geïnformeerd."*

3.8. De mogelijkheid om gegevens aan buitenlandse diensten te verzoeken of te ontvangen is niet expliciet in de Wiv 2002 geregeld, maar wordt verondersteld in artikel 59 Wiv 2002. Blijkens de parlementaire geschiedenis van de Wiv 2002 is het voor de diensten wenselijk geacht om een zo compleet mogelijk beeld te kunnen krijgen met betrekking tot een bepaald onderwerp om een daarvoor in aanmerking komende dienst te kunnen vragen of hij eventueel informatie over het desbetreffende onderwerp heeft of, indien dat niet het geval is, zijn contacten kan gebruiken om alsnog aan de informatie te komen (*Kamerstukken II 1997/1998, 25 877, nr. 3, p. 73*). Een verzoek van een Nederlandse dienst aan een buitenlandse dienst moet voldoen aan alle criteria die gelden voor gegevensverwerking.

3.9. Artikel 43 Wiv 2002 betreft de verwijdering en vernietiging van gegevens. Ingevolge artikel 43 lid 1 en 3 Wiv 2002 worden de gegevens die, gelet op het doel waarvoor zij worden verwerkt, hun betekenis hebben verloren, verwijderd en worden de verwijderde gegevens vernietigd, tenzij wettelijke regels omtrent bewaring daaraan in de weg staan.

3.10. In de artikelen 47 tot en met 56 Wiv 2002 is de kennisneming van door of ten behoeve van de diensten verwerkte gegevens geregeld. Op grond van deze bepalingen deelt de betrokken minister eenieder op diens aanvraag mede of en zo ja welke hem betreffende persoonsgegevens door of ten behoeve van een dienst zijn verwerkt (artikel 47 Wiv 2002), dan wel of kennis kan worden genomen van andere dan persoonsgegevens betreffende de in de aanvraag vermelde bestuurlijke aangelegenheid (artikel 51 Wiv 2002). Voor zover een aanvraag wordt ingewilligd, stelt de minister de aanvrager zo spoedig mogelijk, doch uiterlijk binnen vier weken na bekendmaking van zijn besluit, in het geval van een aanvraag op grond van artikel 47, in de gelegenheid van zijn gegevens kennis te nemen en, in het geval van een aanvraag op grond van artikel 51 Wiv 2002, in kennis van de desbetreffende gegevens (artikelen 47 lid 2 en 51 lid 2 Wiv 2002). Een besluit tot afwijzing van de aanvraag is een besluit in de zin van de Algemene wet bestuursrecht, waartegen bezwaar en beroep openstaat (artikel 1:3 Algemene wet bestuursrecht).

#### **4. Het geschil**

##### **4.1. Eisers vorderen:**

I. te verklaren voor recht dat de Staat in strijd handelt met het Nederlands recht, in het bijzonder met de Wiv 2002 en/of internationale verdragsverplichtingen, in het bijzonder de artikelen 8 van het Europees Verdrag tot Bescherming van de Rechten van de Mens en de Fundamentele Vrijheden (EVRM) en 7 en/of 8 van het Handvest van de grondrechten van de Europese Unie (het Handvest) en/of 10 EVRM en 11 van het Handvest, door van buitenlandse diensten gegevens te ontvangen en/of te gebruiken die via ongeoorloofde middelen zijn vergaard, zoals met behulp van PRISM of vergelijkbare programma's, waaronder begrepen informatie vergaard door buitenlandse diensten zonder deugdelijke grondslag in de Nederlandse wet;

II. de Staat te verbieden gegevens van buitenlandse diensten te ontvangen en/of te gebruiken die zijn verkregen in strijd met het Nederlandse recht en/of één of meer van de internationale verdragsverplichtingen als bedoeld onder I, en/of van gegevens waarvan niet met zekerheid is vast te stellen dat dit niet het geval is;

III. de Staat te gelasten alle passende maatregelen te treffen om de persoonlijke levenssfeer en/of de vrijheid van nieuwsgaring van eisers te beschermen alsmede - wat betreft de NVSA, NVJ, Internet Society en Privacy First - van degenen wier belangen zij ingevolge hun statuten behartigen, in het bijzonder door:

i. betrokkenen over wie de Staat gegevens heeft ontvangen van buitenlandse diensten, zulks in strijd met het Nederlands recht en/of één of meer van de internationale verdragsverplichtingen als bedoeld onder I, althans gegevens waarvan niet met zekerheid is vast te stellen dat dit niet het geval is, binnen drie maanden na betekening van het te dezen wijzen vonnis daarover zoveel mogelijk schriftelijk te informeren, in ieder geval over de betreffende periode, de aard en de hoeveelheid gegevens, de doeleinden waarvoor de gegevens zijn verzameld alsmede, desverzocht door de betrokkenen, van de gegevens een kopie aan de betrokkenen te verstrekken;

ii. betrokkenen de mogelijkheid te bieden uitsluitel te verkrijgen omtrent het al dan niet door de Staat hebben ontvangen van gegevens betreffende hun persoon van buitenlandse diensten, zulks in strijd met het Nederlands recht en/of één of meer van de internationale verdragsverplichtingen als bedoeld onder I, althans gegevens waarvan niet met zekerheid is vast te stellen dat dit niet het geval is, een en ander binnen twee weken na betekening van het te dezen te wijzen vonnis; en/of

iii. gegevens betreffende betrokkenen die de Staat heeft ontvangen van buitenlandse diensten, zulks in strijd met het Nederlands recht en/of één of meer internationale verdragsverplichtingen als bedoeld onder I, althans gegevens waarvan niet met zekerheid vast te stellen dat dit niet het geval is, binnen drie maanden na betekening van het te dezen wijzen vonnis te wissen;

IV. de Staat te veroordelen tot het betalen van een onmiddellijk opeisbare en niet voor matiging vatbare dwangsom van telkens € 50.000,-- ineens voor iedere niet-nakoming van enig onderdeel van de onder II en III omschreven bevelen/veroordelingen, alsmede € 50.000,-- voor iedere dag dat deze niet-nakoming voortduurt, zulks met een maximum van € 1.000.000,--;

V. de Staat in de kosten van deze procedure te veroordelen.

4.2. Eisers leggen aan hun vorderingen onrechtmatig handelen van de Staat ten grondslag. Zij betrekken - zakelijk en samengevat weergegeven - de volgende stellingen.

- 
- De af luister praktijken van de Amerikaanse en Britse veiligheidsdiensten zijn onverenigbaar met de bescherming van de bescherming van de persoonlijke levenssfeer en de communicatievrijheid, zoals gewaarborgd in de artikelen 8 EVRM, 7 en 8 van het Handvest, 10 EVRM en 11 van het Handvest en vergelijkbare verdragsregels zoals neergelegd in de artikelen 17 en 19 IVBPR.
  - De Staat schendt de genoemde internationale verdragsbepalingen door - al of niet op verzoek - gegevens te ontvangen en te gebruiken die door buitenlandse diensten in strijd met die bepalingen zijn verkregen. Artikel 59 Wiv 2002 biedt volgens eisers daarvoor, gelet op de rechtspraak van het EHRM, een onvoldoende met waarborgen omklede wettelijke basis. De wet voorziet niet in de minimumwaarborgen die artikel 8 EVRM eist voor een gerechtvaardigde inbreuk op de persoonlijke levenssfeer. Ook artikel 1 sub f in verbinding met de artikelen 12 en 17 Wiv 2002 biedt een onvoldoende wettelijke basis voor het ontvangen van gegevens van buitenlandse diensten. Verder ontbreekt de noodzaak tot het ontvangen van gegevens door de diensten van buitenlandse diensten voor zover die gegevens zijn verkregen door een schending van grondrechten. Het is aan de Staat om te onderbouwen waarom het noodzakelijk is dat niet kan worden geïnformeerd naar de herkomst van verkregen informatie en waarom de samenwerking niet op een minder ingrijpende manier kan worden gerealiseerd. In de artikelen 7 en 8 van het Handvest zijn het recht op eerbiediging van het privéleven, respectievelijk het recht op bescherming van persoonsgegevens en in artikel 11 is het recht op vrijheid van meningsuiting en informatie verankerd. Het Handvest kent een vergelijkbare beperkingentoets als het EVRM.
  - Het ontvangen en het gebruiken van dergelijke gegevens door de Staat is in strijd met de Wiv 2002. Voor zover die gegevens zijn ontvangen na een daartoe strekkend verzoek van de diensten, is dit in strijd met het uitgangspunt dat de Nederlandse overheid uitsluitend om de inzet van bevoegdheden door een buitenlandse dienst mag verzoeken die de Nederlandse overheid zelf ook bezit, met inachtneming van de vereisten van noodzakelijkheid, proportionaliteit en subsidiariteit die aan de inzet van die bevoegdheid zijn gesteld. Bovendien zijn de Nederlandse diensten onderworpen aan de grond- en mensenrechten die zijn neergelegd in de Grondwet en internationale verdragen die door Nederland zijn geratificeerd, op grond waarvan voor het ontvangen en gebruiken van gegevens sprake moet zijn voor een voorzienbare wettelijke basis. De Wiv 2002 biedt deze niet.
  - De Staat schiet tekort in de op hem op grond van de artikelen 8 en 10 EVRM rustende positieve verplichting om actief maatregelen te nemen om respectievelijk de persoonlijke levenssfeer van zijn burgers en de vrije nieuwsgaring te beschermen. De Staat is op grond van zijn positieve verplichting in ieder geval gehouden om burgers over wie informatie is ontvangen van buitenlandse diensten die in strijd met de artikelen 8 en 10 zijn verkregen daarover te informeren. Voorts moet de Staat personen de mogelijkheid bieden om uitsluitel te verkrijgen over de vraag of gegevens over hen in strijd met artikel 8 en 10 EVRM zijn verkregen. Tot slot moet de Staat ten minste maatregelen nemen om ervoor te zorgen dat dergelijke gegevens worden gewist. De verplichtingen tot het informeren, het geven van inzage en het vernietigen van gegevens zijn algemene beginselen van databescherming. De Dataprotectierichtlijn en de Wet bescherming persoonsgegevens zijn, naar analogie, van belang voor de beoordeling van de hier bedoelde positieve verplichtingen van de Staat.

4.3. De Staat voert verweer.

4.4. Op de stellingen van partijen wordt hierna, voor zover van belang, nader ingegaan.



## 5. De beoordeling

### *Ontvankelijkheid*

5.1. De Staat beroept zich op de niet-ontvankelijkheid van de vijf natuurlijke personen (in de kop van dit vonnis aangeduid als eisers sub 1 tot en met 5) en van de rechtspersonen de NVSA en de NVJ (eisers sub 6 en 7) die de Staat in deze zaak in rechte hebben betrokken. Privacy First en Internet Society Nederland (eisers sub 8 en 9) dienen volgens de Staat niet-ontvankelijk te worden verklaard in hun vordering om de Staat te gelasten passende maatregelen te treffen (zoals in 4.1., onder III weergegeven). De rechtbank overweegt als volgt.

### *Eisers 1 tot en met 5*

5.2. Op grond van artikel 3:303 van het Burgerlijk Wetboek (BW) komt zonder voldoende belang niemand een rechtsvordering toe. Gelet op het karakter en de inhoud van de activiteiten waarop de eisende partijen-natuurlijke personen zich toeleggen, in samenhang gezien met de omstandigheid dat deze eisende partijen nationaal en internationaal in meer of mindere mate bekendheid genieten op het terrein waarop zij werkzaam zijn, acht de rechtbank aannemelijk dat deze eisers, meer dan de gemiddelde burger in Nederland, de verdenking op zich kunnen laden dat zij door hun activiteiten een gevaar voor de nationale veiligheid zouden kunnen opleveren en derhalve op grond van de Wiv 2002 onderwerp zouden kunnen zijn van onderzoek door de diensten. Daaruit volgt dat niet kan worden uitgesloten dat de diensten ter uitvoering van dit onderzoek met betrekking tot hen gegevens verwerken en dus ook verzamelen. De rechtbank acht voor de ontvankelijkheid van deze eisers in de onderhavige procedure niet van belang of dit werkelijk het geval is. Voorts neemt zij in aanmerking dat het enkele bestaan van de Wiv 2002, waarin is voorzien in de mogelijkheid voor de diensten om in het geheim gegevens te verzamelen en samen te werken met buitenlandse diensten, voor eenieder het risico in zich heeft dat gegevens verzameld worden op grond van de Wiv 2002 (vgl. Europese Hof voor de Rechten van de Mens (EHRM) 29 juni 2006, app. no. 54934/00 (*Weber and Saravia v. Germany*, par. 78)). Gelet hierop en gelet op artikel 6 EVRM, welke bepaling het recht op toegang tot de rechter waarborgt, hebben eisers naar het oordeel van de rechtbank voldoende feiten gesteld voor de conclusie dat zij een voldoende, concreet en eigen belang bij hun vorderingen tegen de Staat hebben. De rechtbank verwierpt derhalve het verweer van de Staat dat deze eisers niet in hun vorderingen kunnen worden ontvangen.

### *De NVSA en de NVJ*

5.3. Met de wettelijke regeling van de collectieve actie zoals bepaald in artikel 3:305a BW is onder meer beoogd een effectieve en efficiënte rechtsbescherming ten behoeve van de belanghebbenden te bevorderen. Naar het oordeel van de rechtbank behartigen de NVSA en de NVJ blijkens hun statutaire doelstellingen, anders dan de Staat betoogt, ook de belangen waarvoor zij in deze procedure opkomen. De NVSA behartigt (in ieder geval) de gebundelde belangen van haar leden, zijnde individuele strafrechtadvocaten, waaronder mede begrepen is het belang van Nooitgedagt, en heeft tot doel al datgene te doen wat voor goed functioneren van een verdediging in strafzaken dienstig is. De NVJ behartigt eveneens (in ieder geval) de gebundelde belangen van haar leden, zijnde individuele journalisten, waaronder dat van De Winter, en heeft tot doel onder meer te waken en waar nodig te strijden voor persvrijheid en het recht op informatie van de burgers. Nu de eerbiediging van het privéleven, waaronder mede begrepen wordt de bescherming van correspondentie en communicatie tussen raadsman en cliënt, een essentieel onderdeel vormt van het goed

functioneren van een verdediging in strafzaken en de NVSA met haar vorderingen nu juist de bescherming van die grondrechten van de strafrechtadvocaten wier belangen zij behartigt op grond van dit grondrecht beoogt te bewerkstelligen, kan de NVSA in haar vorderingen worden ontvangen. Ook de NVJ kan in haar vorderingen worden ontvangen, aangezien de persvrijheid en het recht op informatie van burgers onderdeel zijn van het recht op bescherming van de vrijheid van meningsuiting en de NVJ met haar vorderingen op grond van dit grondrecht de bescherming van journalisten wier belangen zij behartigt, beoogt te bewerkstelligen.

*Het gevorderde gebod tot het nemen van passende maatregelen*

5.4. De rechtbank verwerpt ten slotte het betoog van de Staat dat Privacy First en Internet Society Nederland, gelet op de artikelen 47 e.v. Wiv 2002, niet-ontvankelijk moeten worden verklaard in hun vordering om de Staat te gelasten om passende maatregelen te treffen. De omstandigheid dat de Wiv 2002 bepalingen bevat op grond waarvan een aanvraag kan worden ingediend om kennis te nemen van persoonsgegevens en andere gegevens en dat individuele belanghebbenden bij een negatief besluit van de betrokken minister hun bezwaren aan de orde kunnen stellen in een met voldoende waarborgen omklede bestuursrechtelijke rechtsgang, staat in het onderhavige geval niet in de weg aan de ontvankelijkheid van deze rechtspersonen in de genoemde vordering III. De rechtbank overweegt dat Privacy First en Internet Society naar haar oordeel een eigen belang behartigen en niet slechts optreden ter behartiging van de gebundelde belangen van individuele belanghebbenden. Niet aan de orde is een situatie als in de zaak die heeft geleid tot het arrest van de Hoge Raad van 9 juli 2010, NJ 2012, 241 m.nt. H.J. Snijders. In de statuten van Privacy First is met zoveel woorden vermeld dat Privacy First zich in de eerste plaats ten doel stelt het “*behouden en bevorderen van het recht op privacy*”, hetgeen zij beoogt te realiseren door onder meer het in rechte optreden voor “*alle burgers in Nederland ter bescherming van dit algemene belang*”. De belangen die Privacy First behartigt, overstijgen naar het oordeel van de rechtbank dan ook de gebundelde belangen van individuele belanghebbenden. In de statuten van Internet Society Nederland is niet uitdrukkelijk vermeld dat zij mede optreedt voor alle burgers in Nederland ter bescherming van het algemeen belang van het recht op privéleven. Niettemin ligt naar het oordeel van de rechtbank in de doelstelling van Internet Society Nederland, onder meer inhoudende “*het stimuleren van gebruik en toepassingen van het internet in Nederland en het participeren in de evolutie en ontwikkelingen van het internet in de internationale context*”, en de algemene formulering van die doelstelling besloten dat deze mede strekt tot bescherming van het recht op privéleven van alle internetgebruikers in Nederland. Hier komt bij dat haar optreden in rechte blijkens de statuten niet beperkt is tot de behartiging van de belangen van leden. De rechtbank neemt gelet hierop aan dat ook in het geval van Internet Society Nederland niet kan worden gezegd dat zij slechts optreedt ter behartiging van de gebundelde belangen van individuele belanghebbenden.

5.5. Daarnaast acht de rechtbank van belang dat de vordering van eisers de Staat te gelasten passende maatregelen te treffen niet de onverbindendheid van de Wiv 2002 betreft. Het gevorderde gebod is gebaseerd op gesteld onrechtmatig handelen van de Staat wegens schending van de gestelde positieve verplichting van de Staat op grond van de artikelen 8 en 10 EVRM. In ieder geval voor zover het gevorderde gebod strekt tot het wissen van gegevens kan er bezwaarlijk van worden uitgegaan dat door individuele belanghebbenden langs de bestuursrechtelijke weg de maatregelen zoals in de onderhavige procedure gevorderd in rechte kunnen worden afgedwongen. De Wiv 2002 voorziet niet in de

---

mogelijkheid tot het wissen van gegevens op een daartoe strekkende aanvraag. De bestuursrechtelijke rechtsgang levert dus een rechtstekort op, waarin de burgerlijke rechter dient te voorzien.

5.6. Op grond van de genoemde, uiteenlopende redenen kan in dit geval niet worden aangenomen dat, met het oog op een behoorlijke taakverdeling tussen de bestuursrechter en de burgerlijke rechter, het gestelde onrechtmatige handelen van de Staat dat ten grondslag ligt aan de desbetreffende vorderingen, alleen door de betrokken burger zelf kan worden aangevochten in het kader van een bestuursrechtelijke procedure na een (daartoe uitgelokt) afwijzend besluit van de betrokken minister op een aanvraag in de zin van de artikelen 47 of 51 Wiv 2002. Een en ander leidt tot de conclusie dat Privacy First en Internet Society Nederland ook in deze vordering kunnen worden ontvangen.

### ***Inhoudelijke beoordeling***

#### ***Leeswijzer inhoudelijke beoordeling***

5.7. De opbouw van de inhoudelijke beoordeling van de rechtbank is als volgt. In enige inleidende opmerkingen zal de rechtbank uiteenzetten wat de kernvraag is die zij in deze zaak moet beantwoorden. Daarna zal zij in het licht van de vorderingen van eisers haar beoordelingskader bepalen en ingaan op de feitelijke uitgangspunten die zij bij haar beoordeling in acht neemt. Vervolgens zal zij beoordelen of de Staat in verband met de ontvangst en het gebruik door de diensten van gegevens van buitenlandse diensten handelt in strijd met internationale verdragsverplichtingen en/of de Wiv 2002, zoals eisers stellen. Dan komt aan de orde of op de Staat een positieve verplichting rust, zoals eisers tevens betogen. De inhoudelijke beoordeling mondt uit in een slotsom (zie in 5.47. e.v.).

#### ***Inleidende opmerkingen***

5.8. De inzet van eisers in deze procedure is tweërlei. In de eerste plaats beogen eisers dat een einde wordt gemaakt zowel aan de ontvangst als aan het gebruik van gegevens door de diensten die betrekking hebben i) op burgers in Nederland en ii) in strijd met Nederlandse rechtsbeginselen zijn verkregen. In de tweede plaats willen zij dat maatregelen worden getroffen om de persoonlijke levenssfeer en communicatievrijheid van burgers in Nederland zoveel mogelijk te beschermen, onder meer door diegenen van wie gegevens door de NSA of andere (buitenlandse) diensten door middel van een ongeoorloofde inmenging op hun privéleven zijn verkregen, daarover te informeren.

5.9. Eisers komen op voor grondrechten op bescherming van de persoonlijke levenssfeer, waaronder de vrijheid van communicatie tussen de (strafrecht)advocaat en zijn cliënt, en op de vrijheid van meningsuiting, nieuwsgaring en informatie. Deze grondrechten zijn fundamenteel van aard en strekken tot bescherming van de betrokken eisers als individu. Het EVRM beschermt het individu tegen ongeoorloofde inbreuken van de overheid op die rechten. Nederland is gebonden aan het EVRM.

5.10. Internationale samenwerking dient, uit het oogpunt van nationale veiligheid, het algemeen belang van burgers in Nederland. Het staat vast dat de Nederlandse diensten verzamelingen (ruwe) gegevens uitwisselen met buitenlandse diensten, waaronder de NSA. Inherent aan die samenwerking is de praktijk (de *modus operandi*) dat inlichtingen- en veiligheidsdiensten elkaar niet plegen te informeren over hun bronnen en dat ten aanzien van de uitwisseling van die informatie het wederkerigheidsbeginsel (*quid pro quo*) geldt. Dit betekent dat de diensten in het kader van de uitwisseling van gegevens in de regel niet weten

---

op welke wijze de gegevens die zij van buitenlandse diensten ontvangen en vervolgens gebruiken, zijn verzameld. Hoewel buitenlandse diensten zijn gebonden aan de voor hen geldende internationale verdragsverplichtingen en wet- en regelgeving kan, gelet op de praktijk van samenwerking tussen inlichtingen- en veiligheidsdiensten, niet worden uitgesloten dat die gegevens door buitenlandse diensten zijn verzameld in strijd met op Nederland rustende internationale verdragsverplichtingen, zoals die op grond van artikel 8 EVRM.

5.11. De kernvraag die de rechtbank gelet op het vorenstaande moet beantwoorden, betreft dan ook de reikwijdte van de bescherming van het individuele belang van eisers en, zoals zij stellen, van alle burgers in Nederland, dat gemoeid is met de bescherming van hun grondrechten in het licht van het algemene belang van de burgers in Nederland dat gemoeid is met het bestaan van internationale samenwerking tussen de diensten en buitenlandse diensten. Daarbij is de vraag aan de orde of de Staat (de diensten) tegenover eisers onrechtmatig handelt door het ontvangen en eventueel gebruiken van gegevens van buitenlandse diensten die zijn vergaard op een wijze die mogelijk in strijd is met de hier geldende regels van verdragen en de nationale wetgeving (Wiv 2002). De vorderingen zijn algemeen geformuleerd en gaan uit van de gedachte dat reeds de mogelijkheid dat dit het geval is, een onrechtmatige daad jegens eisers oplevert.

*Beoordelingskader*

5.12. De vorderingen van eisers zijn gebaseerd op de stelling dat de Staat van buitenlandse diensten gegevens ontvangt en/of gebruikt die via ongeoorloofde middelen zijn vergaard, zoals met behulp van 'PRISM' of vergelijkbare programma's, waaronder begrepen informatie die is vergaard door buitenlandse diensten zonder deugdelijke grondslag in de Nederlandse wet.

5.13. Hieruit volgt dat de rechtbank dient te beoordelen of *de ontvangst en het gebruik* door de Staat van gegevens *van buitenlandse diensten* die door die diensten zijn vergaard op de door eisers gestelde wijze, in strijd zijn met de Wiv 2002 en/of internationale verdragsverplichtingen, en of in verband met de ontvangst en het gebruik van deze gegevens op de Staat een positieve verplichting rust. De ontvangst en het gebruik van deze gegevens zijn gebaseerd op artikel 59 lid 1 Wiv 2002. Buiten beschouwing blijft dus de verstrekking van gegevens in de zin van de Wiv 2002 aan buitenlandse diensten en het verlenen van ondersteuning aan deze diensten door de Staat op grond van de artikelen 59 leden 2 en 4 Wiv 2002. Eveneens laat de rechtbank buiten beschouwing de ontvangst en het gebruik van gegevens door de Staat op basis van de inzet van bijzondere bevoegdheden die aan de diensten in de artikelen 20-29 Wiv 2002 zijn toegekend.

5.14. De vorderingen van eisers zijn voorts, gezien hun inzet van deze procedure, algemeen geformuleerd en verstrekkend van aard. Eisers hebben de reikwijdte van hun vorderingen ter zitting nader toegelicht met de stelling dat het gestelde onrechtmatig handelen van de Staat eenieder treft. Zij hebben gesteld dat de NSA en de GCHQ op elk moment in het leven van eenieder kan binnendringen en dat iedereen zich iedere dag blootstelt aan surveillance (toezicht) en dat het aan de Staat is om daartegen bescherming te bieden, niet om de burgers op te offeren voor een goede vertrouwensband met de Amerikanen. Een en ander brengt mee dat de rechtbank moet beoordelen of de genoemde ontvangst en het gebruik van gegevens van buitenlandse diensten door de Staat (de diensten) *zonder meer, derhalve onder alle omstandigheden*, in strijd zijn met de Wiv 2002 en met

internationale verdragsverplichtingen. Gelet op de hiervoor genoemde kernvraag komt dit neer op de beoordeling of, als het ware, een “hek aan de grens” moet worden gezet.

*Feitelijke uitgangspunten*

5.15. Eisers doelen blijkens de stukken van het geding en het verhandelde ter comparitie met de term ‘ongeoorloofde middelen’ op tal van surveillanceprogramma’s, waaronder ‘PRISM’ en ‘Tempora’, waarvan de NSA respectievelijk de GCHQ gebruik maken om gegevens te verzamelen. Zij kwalificeren de gestelde Amerikaanse en Britse werkwijze en de schaal waarop met die werkwijze gegevens worden verzameld als spionagepraktijken met als motto: ‘collect it all’. De diensten krijgen, aldus eisers, via buitenlandse diensten de beschikking over gegevens die zij zelf nooit hadden mogen vergaren, hetgeen volgens hen neerkomt op het ‘witwassen van illegale data’.

5.16. De Staat heeft zich hiertegen verweerd met de stelling dat er geen aanwijzingen zijn dat buitenlandse diensten informatie aan de diensten hebben verschaft, die door die buitenlandse diensten zijn verzameld door middel van een inbreuk op de Nederlandse rechtssfeer of soevereiniteit. Voorts heeft de Staat betoogd, met een beroep op het rapport van de CTIVD van 5 februari 2014, dat er geen aanwijzingen zijn dat buitenlandse diensten met medewerking van de AIVD of de MIVD zelfstandig toegang hebben gekregen tot Nederlandse telefoon- of internetverbindingen, dat er geen sprake is van het stelselmatig door de diensten buiten de Nederlandse wet- en regelgeving om verwerven van persoonsgegevens of andere gegevens en ten slotte dat er geen aanwijzingen zijn dat de AIVD of de MIVD expliciet verzoeken aan buitenlandse diensten hebben gedaan om bevoegdheden in te zetten die volgens de Nederlandse wet- en regelgeving niet zijn toegestaan (de eerdergenoemde U-bochtconstructie). Deze verweren zijn onweersproken gebleven, zodat de rechtbank bij haar beoordeling de door de Staat genoemde feitelijke constatering tot uitgangspunt neemt. Voor zover de vorderingen van eisers zijn gebaseerd op de stelling dat de Staat in strijd handelt met de Wiv 2002, los van artikel 8 (en artikel 10) EVRM, stuiten die vorderingen hierop af.

5.17. De uitwisseling van verzamelingen (ruwe) gegevens tussen de diensten en buitenlandse diensten vindt plaats (zie hiervoor in 2.26.) binnen bepaalde hechte samenwerkingsrelaties van de diensten met buitenlandse diensten en al dan niet op structurele basis. Blijkens het rapport van de CTIVD van 5 februari 2014 betreft het hier gegevens die zijn verkregen door de inzet van bijzondere bevoegdheden die nog niet op relevantie zijn beoordeeld. Daarbij kan het gaan om zowel metagegevens als de eigenlijke, inhoudelijke communicatie. In verband met de uitwisseling van deze verzamelingen gegevens heeft de CTIVD, over de ontvangst van die gegevens, in haar rapport onder meer overwogen: “*wel is de Commissie gestuit op de situatie dat sommige buitenlandse diensten waarmee de Nederlandse diensten samenwerken de bevoegdheid hebben om ongericht kabelgebonden communicatie te intercepteren. Dit valt voor hen onder onder het begrip sigint. De Nederlandse diensten beschikken niet over deze bevoegdheid. De Commissie constateert dat wanneer de AIVD en de MIVD sigint van buitenlandse diensten ontvangen, hetgeen met enige regelmaat voorkomt, zij daardoor wellicht ook gegevens ontvangen die het resultaat zijn van kabelgebonden interceptie.*” Voorts heeft de minister van Defensie na de Snowden-onthullingen in de Tweede Kamer op vragen geantwoord dat zij niet kan uitsluiten dat er ooit gebruikgemaakt wordt van gegevens die via het programma ‘PRISM’ bij de diensten zijn beland.

5.18. Gelet op het vorenstaande neemt de rechtbank tot feitelijk uitgangspunt dat de diensten in het kader van de uitwisseling van (ruwe) gegevens met buitenlandse diensten *mogelijk* mede gegevens ontvangen die het resultaat zijn van de inzet van bevoegdheden van die buitenlandse diensten waarover de diensten op grond van de Wiv 2002 zelf niet beschikken. Daaronder kunnen zich ook gegevens bevinden die door de buitenlandse diensten via 'PRISM' zijn verzameld.

*Schending internationale verdragsverplichtingen en Wiv 2002?*

5.19. De ontvangst en, daaruit voortvloeiend, ook het eventuele gebruik van gegevens die zijn vergaard door buitenlandse diensten, is gebaseerd op artikel 59 lid 1 Wiv 2002: "*De hoofden van de diensten dragen zorg voor het onderhouden van verbindingen met daarvoor in aanmerking komende inlichtingen- en veiligheidsdiensten van andere landen.*" De selectie van buitenlandse diensten vindt plaats, zoals de Staat onweersproken heeft gesteld, op basis van een aantal criteria, te weten de democratische inbedding van de desbetreffende dienst en respect voor mensenrechten, de professionaliteit en betrouwbaarheid en het karakter van de dienst. Ook internationale verplichtingen kunnen een rol spelen. Ter zitting hebben eisers gesteld dat het hun in deze zaak niet gaat om de samenwerking met buitenlandse diensten als zodanig, maar om de grenzen die in het kader van deze samenwerking in acht moeten worden genomen. Nu eisers hun stellingen toespitsen op de samenwerking met de NSA, zal de rechtbank hierna in het bijzonder op die samenwerking ingaan. Nu het eisers niet om de samenwerking met de NSA als zodanig is te doen en zij onvoldoende feiten hebben gesteld die nopen tot de conclusie dat de NSA niet aan de genoemde selectiefactoren voldoet, is uitgangspunt dat de diensten op zichzelf mogen samenwerken met de NSA. Dit geldt naar het oordeel van de rechtbank ook indien Nederland deel zou uitmaken van de zogenoemde 'Nine Eyes', waarbij de rechtbank in het midden laat of dit het geval is.

5.20. Bij de bepaling van de grenzen die in het kader van die samenwerking door de Staat in acht moeten worden genomen, is naar het oordeel van de rechtbank allereerst van belang dat de buitenlandse diensten bij het verzamelen van gegevens gebonden zijn aan de voor hen geldende nationale wet- en regelgeving en internationale verdragsverplichtingen. In het geval van de VS gaat het hier, voor zover relevant, om het Internationaal Verdrag inzake Burgerrechten en Politieke Rechten (IVBPR). De artikelen 17 en 19 van het IVBPR betreffen, zoals ook eisers hebben aangehaald, het recht op eerbiediging van de persoonlijke levenssfeer en het recht op vrijheid van meningsuiting en het vergaren van informatie. In het algemeen mogen de diensten er naar het oordeel van de rechtbank op vertrouwen dat buitenlandse diensten die voldoen aan de selectiefactoren voor samenwerking de voor hen geldende nationale wet- en regelgeving en internationale verdragsverplichtingen respecteren. Ook het omgekeerde is het geval.

5.21. De vraag die dan rijst, is of hiermee kan worden volstaan. In de Amerikaanse wet- en regelgeving zijn de bevoegdheden van de NSA tot het verzamelen van gegevens neergelegd. Op grond van Section 702 van de Foreign Intelligence Surveillance Act (FISA) zijn de Attorney General en de Director of National Intelligence bevoegd voor een periode tot een jaar buitenlands inlichtingenmateriaal te verzamelen over personen ten aanzien van wie een redelijk vermoeden bestaat dat zij zich buiten de Verenigde Staten bevinden. De uitoefening van deze bevoegdheid is aan voorwaarden gebonden en er moet een machtiging worden verleend voordat de bevoegdheid kan worden uitgeoefend. Op grond van Section 215 van de US Patriot Act kunnen Amerikaanse inlichtingen- en veiligheidsdiensten, met het oog op onderzoek dat geen betrekking heeft op een Amerikaans staatsburger of in het

---

kader van onderzoek naar internationaal terrorisme of spionage, inlichtingenmateriaal, waaronder metadata, verzamelen door het uitvaardigen van een zogenoemde '*FISC Document Production Order*'. Hiervoor is een machtiging van de Foreign Intelligence Surveillance Court (FISC), vereist. Het gebruik van de aan de NSA toekomende bevoegdheden tot het vergaren van gegevens is achteraf onderworpen aan parlementaire controle en aan het toezicht van de interne '*Inspector General*'. Voorafgaand aan de inzet van die bevoegdheden vindt controle door de FISC plaats. Naar het oordeel van de rechtbank kan, gegeven deze wet- en regelgeving en het daarin vervatte systeem van toezicht op de naleving ervan, *niet in algemene zin* gezegd worden, zoals eisers stellen, dat de diensten in het geval van de ontvangst en het gebruik van gegevens van de NSA, in strijd met artikel 8 EVRM handelen. De omstandigheid dat de rechtspraak in de VS divergeert ten aanzien van de vraag of de vergaring van inlichtingenmateriaal door de NSA op basis van Section 702 FISA en Section 215 van de US Patriot in overeenstemming is met het Vierde Amendement van de Amerikaanse grondwet, alsmede dat uit het onderzoek van de EU-VS-expertgroep naar voren is gekomen dat de eisen in de Amerikaanse wet- en regelgeving om inlichtingen te vergaren met betrekking tot personen die geen Amerikaans staatsburgers zijn lager zijn dan die voor Amerikaanse staatsburgers, acht de rechtbank onvoldoende voor een andere conclusie.

5.22. Het vorenstaande laat onverlet dat niet bekend is op welke wijze de NSA gegevens verzamelt. A fortiori bestaat daarover geen zekerheid. Er moet derhalve rekening worden gehouden met de mogelijkheid dat de diensten in het kader van de internationale samenwerking gegevens ontvangen die zijn verzameld op een wijze die niet in overeenstemming is met het bepaalde in artikel 8 EVRM. Van belang in dit verband is ook (zie hiervoor in 2.30.) dat sprake is van een beduidend verschil in interpretatie tussen de VS en EU-landen (en overigens ook tussen EU-landen onderling) van het begrip verwerking ("*processing*") van (persoons)gegevens door veiligheidsdiensten, waarbij in de VS de initiële verzameling van (persoons)gegevens niet steeds onder die verwerking valt en op het moment van de verzameling weliswaar sprake is van zekere waarborgen, maar aanvullende waarborgen bestaan vanaf het moment van de verdere verwerking ervan. In sommige opzichten biedt de Amerikaanse regelgeving, zoals blijkt uit het vorenstaande, minder waarborgen ten opzichte van degenen die geen staatsburger van de VS zijn. De omstandigheid dat er geen aanwijzingen zijn dat de diensten stelselmatig buiten de Nederlandse wet- en regelgeving om persoonsgegevens en andere gegevens verwerven en dat er evenmin aanwijzingen zijn dat zij expliciet verzoeken aan buitenlandse diensten hebben gedaan om bevoegdheden in te zetten die volgens de Nederlandse wet- en regelgeving niet zijn toegestaan (de U-bochtconstructie) doet er niet aan af dat niet kan worden uitgesloten dat de diensten gegevens ontvangen die in de VS in strijd met artikel 8 EVRM zijn vergaard en dat zij deze gegevens ook gebruiken.

5.23. Dit zo zijnde, rijst de vraag of artikel 8 EVRM vereist dat de nationale wetgeving voorziet in de door eisers gestelde waarborgen ter bescherming van hun grondrechten. De rechtbank stelt vast dat artikel 59 lid 1 Wiv een wettelijke basis biedt voor samenwerking tussen de diensten en buitenlandse inlichtingen- en veiligheidsdiensten en, gelet op de wetsgeschiedenis van de Wiv 2002, tevens voor de ontvangst en het gebruik van gegevens door de diensten die door de buitenlandse diensten zijn vergaard. Volgens eisers moet op grond van artikel 8 EVRM in de Wiv 2002 evenwel (in ieder geval) gewaarborgd zijn in welke gevallen welk type gegevens mag worden ontvangen, welke procedure daarbij moet worden gevolgd, hoe lang de gegevens mogen worden bewaard en welke

---

voorzorgsmaatregelen de diensten moeten nemen, bij gebreke waarvan volgens hen zonder meer sprake is van een ongeoorloofde inbreuk op de persoonlijke levenssfeer van een individu.

5.24. In dit verband verdient eerst opmerking dat artikel 8 EVRM het individu beschermt tegen willekeurige inbreuken van de overheid op onder meer de grondrechten op respect voor zijn privéleven en zijn correspondentie. Deze rechten hangen nauw samen met de persoonlijke levenssfeer, de individuele en relationele vrijheid en de persoonlijke autonomie. De bescherming van deze klassieke grondrechten door het EVRM, waarbij wordt uitgegaan van het individuele belang en persoonlijke schade, biedt geen pasklaar antwoord op de vragen die uit privacy-oogpunt rijzen in verband met grootschalige verzameling van gegevens in bulk. Die verzameling betreft immers per definitie niet het individu, maar, zoals eisers ter zitting ook naar voren hebben gebracht, in beginsel “eenieder”. Het antwoord op de vraag of sprake is van een ongeoorloofde inbreuk op de grondrechten van artikel 8 EVRM hangt evenwel in sterke mate af van de concrete omstandigheden van het geval, zoals hierna zal worden uiteengezet aan de hand van de rechtspraak van het EHRM. Dit aspect moet niet uit het oog worden verloren bij de beantwoording van de vraag welke waarborgen de nationale wetgeving op grond van het EVRM moet bieden ter bescherming van de persoonlijke levenssfeer in verband met de ontvangst en het gebruik van verzamelingen gegevens van buitenlandse diensten. Anders dan eisers lijken te menen, kan voorts het recht op bescherming van de persoonlijke levenssfeer niet gelijk worden gesteld aan het recht op bescherming van persoonsgegevens zoals neergelegd in artikel 8 van het Handvest. Voor een beroep op bescherming van het recht van persoonsgegevens zoals neergelegd in het Handvest is voldoende dat sprake is van de verwerking van gegevens die te herleiden zijn tot een te identificeren individu. Het EHRM maakt onderscheid tussen gegevens die wel en gegevens die niet worden beschermd door artikel 8 EVRM, waarbij het EHRM toetst of het privéleven van een individu door de verwerking van de gegevens wordt geraakt (vgl. EHRM 25 september 2001, app. no. 44787/98 (*P.J. and J.H. v. The United Kingdom*), par. 42). Ook de mate van bescherming die in het Handvest aan persoonsgegevens wordt toegekend, is ruimer dan die in het EVRM met betrekking tot het recht op bescherming van de persoonlijke levenssfeer. Ingevolge artikel 8 lid 2 van het Handvest moeten persoonsgegevens eerlijk worden verwerkt, voor bepaalde doeleinden en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet. Bovendien heeft eenieder recht op toegang tot de over hem verzamelde gegevens en op rectificatie daarvan en ziet een onafhankelijke autoriteit toe op de naleving van deze regels. Die bescherming kan, zoals ook hierna aan de orde zal komen, niet in gelijke mate worden ontleend aan het EVRM. Overigens is het Handvest van toepassing op de lidstaten, uitsluitend wanneer zij het recht van de Unie ten uitvoer leggen (artikel 51 Handvest). Die situatie is in dit geval niet aan de orde.

5.25. Daarnaast is het volgende van belang. Het toepassingsbereik van artikel 8 EVRM strekt zich blijkens de rechtspraak van het EHRM uit tot het verzamelen (ook: intercepteren, of: onderscheppen) en verwerken van metagegevens en het opslaan en verwerken van persoonsgegevens (zie o.a. EHRM 2 augustus 1984, app. no. 8691/79 (*Malone v. The United Kingdom*), par. 84, respectievelijk o.a. EHRM 26 maart 1987, app. no. 9248/81 (*Leander v. Sweden*), par. 48). Volgens vaste rechtspraak is een inbreuk op de persoonlijke levenssfeer van een individu op grond van artikel 8 lid 2 EVRM (slechts dan) gerechtvaardigd indien die inbreuk (1) in overeenstemming is met het recht (“*in accordance*



*with the law*”) en (2) noodzakelijk is in een democratische samenleving (“*necessary in a democratic society*”) voor (3) verwezenlijking van één van de in deze bepaling genoemde doelen, waaronder de nationale veiligheid.

5.26. Het als eerste genoemde vereiste houdt in dat de inmenging een basis moet hebben in de nationale wetgeving en dat deze wetgeving voldoende toegankelijk en voldoende voorzienbaar moet zijn. Het EHRM zwakt de eis van voorzienbaarheid in het kader van geheime surveillance af omdat de inzet van dergelijke geheime maatregelen, wil hij effectief blijven, noodzakelijk gedeeltelijk *onvoorzienbaar* moet blijven (zie het EHRM in zijn uitspraak in de zaak *Malone v. The United Kingdom*, par. 67). Eisers gaan hieraan ten onrechte voorbij. Voldoende is volgens het EHRM dat er een wettelijke basis bestaat die de reikwijdte van een inmenging (of de bevoegdheid hiertoe) en de voorwaarden voor de uitoefening van de discretionaire bevoegdheid hiertoe bepaalt. De wet moet echter wel voldoende duidelijk geformuleerd zijn, opdat zij de burger een voldoende aanwijzing geeft van de omstandigheden waarin en de voorwaarden waaronder de overheden de bevoegdheid hebben een beroep te doen op dergelijke en mogelijk gevaarlijke inmengingen op het recht op respect voor het privéleven en de correspondentie (vgl. ook EHRM 16 februari 2000, app. no. 27798/95 (*Amman v. Switzerland*), par. 44 en 62).

5.27. In zaken die betrekking hebben op geheime surveillance heeft het EHRM een aantal minimumwaarborgen samengevat die de nationale wetgeving op dit terrein moet bevatten om misbruik van bevoegdheden (“*abuses of power*”) te voorkomen. De nationale wetgeving moet volgens het EHRM in ieder geval regels bevatten over: “*the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit for the duration of telephone tapping; the procedure to be followed for examining, using and storing of the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed.*” (zie de eerder genoemde uitspraak van het EHRM in *Weber and Saravia v. Germany*, par. 95). Uit de uitspraak van het EHRM van 1 juli 2008, app. 58243/00 (*Liberty and others v. The United Kingdom*), par. 63, kan worden gedestilleerd dat de geformuleerde minimumwaarborgen niet slechts betrekking hebben op de gerichte interceptie van telecommunicatie tussen individuen, maar tevens op meer ongerichte vormen van interceptie van telecommunicatie, waaronder, in die zaak, het strategisch monitoren van de (inhoud van) telefoongesprekken.

5.28. De rechtbank verwierpt de stelling van eisers dat de lijn die het EHRM in de zaak *Liberty v. The United Kingdom* heeft geformuleerd zonder meer moet worden doorgetrokken naar de verzameling van (ruwe) gegevens in bulk in het kader van internationale samenwerking tussen inlichtingen- en veiligheidsdiensten. Naar het oordeel van de rechtbank valt een dergelijke conclusie niet aan de rechtspraak van het EHRM te ontlelen. De rechtbank laat in het midden of artikel 59 lid 1 Wiv zoals thans geformuleerd onder alle omstandigheden de toets der kritiek van artikel 8 EVRM kan doorstaan. Zodanig verstrekkende waarborgen als eisers voorstaan, eist artikel 8 lid 2 EVRM naar het oordeel van de rechtbank bij de ontvangst en het gebruik van gegevens in het kader van internationale samenwerking zoals door eisers gesteld, evenwel niet. Daartoe is het volgende van belang.

5.29. Geen van de uitspraken van het EHRM betreffende het verzamelen en de verwerking van gegevens heeft betrekking op de uitwisseling van gegevens in het kader van

---

internationale samenwerking. Het EHRM heeft steeds de nationale wetgeving betreffende de inzet van (bijzondere) bevoegdheden van de nationale inlichtingen- en veiligheidsdiensten van de betrokken lidstaat getoetst. Bij internationale samenwerking op het gebied van geheime surveillance bestaat er naar het oordeel van de rechtbank temeer aanleiding voor een bijzondere, dat wil zeggen minder stringente, invulling van de eisen die artikel 8 lid 2 EVRM stelt aan de gerechtvaardigdheid van een inbreuk op de persoonlijke levenssfeer van het individu, in het bijzonder wat betreft de voorzienbaarheid van de nationale wetgeving. Dit, om de volgende redenen.

5.30. In verband met de uitwisseling van gegevens tussen de diensten en buitenlandse diensten geldt allereerst dat deze gegevens worden verzameld door de buitenlandse diensten op basis van de hun toekomende (bijzondere) bevoegdheden. Dit betekent dat het van de waarborgen van de voor die buitenlandse diensten geldende regels afhangt of bij de uitoefening van de bijzondere bevoegdheden van die diensten wordt voldaan aan (het voor de diensten geldende) artikel 8 EVRM. In dit verband is niet van belang of bij de inzet van de bevoegdheden van de buitenlandse diensten sprake is van gerichte of van ongerichte interceptie van telecommunicatie en of die interceptie betrekking heeft op kabelgebonden of op niet-kabelgebonden telecommunicatie. Ook de ongerichte interceptie van kabelgebonden telecommunicatie kan immers, mits met voldoende waarborgen omkleed, aan de voorzienbaarheidstoets van artikel 8 lid 2 EVRM voldoen. Hieruit vloeit voort dat de ontvangst en het gebruik van gegevens door de diensten van buitenlandse diensten die door die diensten zijn vergaard door ongerichte interceptie van kabelgebonden telecommunicatie, op zichzelf niet zonder meer onrechtmatig is, ofschoon hier te lande de Wiv 2002 niet voorziet in de bevoegdheid van de diensten om op die manier inlichtingen te verzamelen. Dit geldt ook voor de inzet van eventuele andere (bijzondere) bevoegdheden waarover die buitenlandse diensten beschikken en de diensten niet.

5.31. Afgezien daarvan is van belang dat in het kader van internationale samenwerking, voor zover in deze procedure relevant, sprake is van de uitwisseling van (ruwe) gegevens in bulk die nog niet op relevantie zijn beoordeeld. Dit betekent dat de data betrekking kunnen hebben zowel op metagegevens als op de inhoud van telecommunicatie. Zoals hiervoor overwogen, valt de verzameling van metagegevens ("metering" in de bewoordingen van het EHRM), voor zover dit plaatsvindt in het kader van geheime surveillance (onderzoek of toezicht), onder de reikwijdte van artikel 8 EVRM. Het verzamelen van metagegevens moet echter, gelet op de aard van die gegevens, worden onderscheiden van het onderscheppen van de inhoud van telecommunicatie, zoals telefoongesprekken, waarvan sprake was in de zaak die heeft geleid tot de uitspraak van het EHRM in de zaak *Malone v. The United Kingdom* (zie par. 84 van die uitspraak van het EHRM en ook de eerdergenoemde uitspraak in *P.J. and J.H. v. The United Kingdom*, par. 42). Het EHRM heeft voorts in zijn uitspraak van 2 september 2010, app. no. 35623/05 (*Uzun v. Germany*), in het geval van geheim toezicht van een verdachte via het Global Position System (GPS), waarbij derhalve gegevens via satellietverbindingen zijn verzameld, de desbetreffende minimumwaarborgen niet van toepassing geacht. Het EHRM acht de strenge standaard zoals in zijn uitspraak inzake *Liberty v. The United Kingdom* geformuleerd niet van toepassing omdat surveillance via GPS, aldus het EHRM, een minder ernstige inbreuk op het privéleven van het individu oplevert dan de interceptie van zijn of haar telefoongesprekken (zie par. 65 en 66 van deze uitspraak). Gelet hierop heeft het EHRM in die uitspraak de meer algemene beginselen van bescherming tegen een willekeurige inbreuk met de grondrechten van artikel 8 EVRM toegepast. Voldoende was volgens het EHRM (par. 63) dat de nationale wetgeving

---

toereikende en effectieve waarborgen biedt tegen een willekeurige inbreuk op de persoonlijke levenssfeer. Deze beoordeling is blijkens deze uitspraak voorts relatief en sterk verweven met de omstandigheden van het geval. Voor toepassing van deze laatste maatstaf, meer dan voor toepassing van de gestelde minimumwaarborgen, is naar het oordeel van de rechtbank ook aanleiding in het geval van de ontvangst van gegevens in bulk, waarbij immers ten tijde van de ontvangst niet bekend is wat de aard van de gegevens is en op welk(e) individu(en) deze gegevens betrekking hebben. Ook als de verzamelingen mogelijk mede betrekking hebben op de inhoud van telecommunicatie (of het strategisch monitoren daarvan) kan de ernst van de inbreuk op het privéleven niet gelijk worden gesteld aan die in de zaken die hebben geleid tot de uitspraken van het EHRM in *Weber and Saravia v. Germany* en *Liberty v. The United Kingdom*.

5.32. Verder moet blijkens de rechtspraak van het EHRM ten aanzien van de eisen die aan de voorzienbaarheid van de wetgeving worden gesteld, worden onderscheiden tussen nationale wetgeving betreffende het verzamelen (intercepteren of onderscheppen) van gegevens enerzijds en het verwerken van gegevens anderzijds. De rechtbank verwijst naar de uitspraak van het EHRM van 25 september 2001, app. no. 44787/98 (*P.G. and J.H. v. The United Kingdom*), par. 46-48). Het verzamelen van gegevens moet, uit het oogpunt van de eisen die het EVRM aan de nationale wetgeving stelt, derhalve worden onderscheiden van andere handelingen die op grond van de Wiv 2002 onderdeel zijn van de verwerking van gegevens, zoals bijvoorbeeld het opslaan, ordenen, raadplegen en samenbrengen en het in onderling verband brengen van gegevens, alsmede het extern verstrekken van gegevens. In hoeverre de uitwisseling van gegevens een inbreuk op de persoonlijke levenssfeer van het individu meebrengt, is met name afhankelijk van wat er met die gegevens gebeurt.

5.33. De conclusie is dat het karakter van de uitwisseling van de verzamelingen gegevens tussen de diensten en buitenlandse diensten, namelijk in bulk en zonder dat deze op relevantie zijn beoordeeld, meebrengt dat de ontvangst van deze gegevens niet aan zulke strenge eisen hoeft te voldoen als eisers voor ogen hebben. De Wiv 2002 bevat voorts voldoende waarborgen voor de verdere verwerking (waaronder het gebruik) van die gegevens. In artikel 12 Wiv 2002 is immers geborgd dat de verwerking van gegevens slechts plaatsvindt voor een bepaald doel en slechts voor zover dat noodzakelijk is voor een goede uitvoering van de Wiv 2002 of de Wet veiligheidsonderzoeken, en ook dat dit in overeenstemming met de Wiv 2002 en op behoorlijke en zorgvuldige wijze geschiedt. In artikel 13 van de Wiv 2002 zijn de categorieën van personen genoemd ten aanzien van wie gegevens kunnen worden verwerkt. Eisers hebben geen feiten gesteld waaruit volgt dat de in de Wiv 2002 vervatte regeling betreffende de verwerking van gegevens niet voldoet aan de bepalingen in het EVRM.

5.34. Eisers werpen de Staat tegen dat de *modus operandi* van inlichtingen- en veiligheidsdiensten, op grond waarvan diensten elkaar niet plegen te informeren over hun bronnen, en het wederkerigheidsbeginsel ten aanzien van de uitwisseling van informatie, waarop de Staat zich beroept, geen valide argumenten vormen voor het ontbreken van de door hen gestelde waarborgen. Die feitelijke praktijk kan naar het oordeel van de rechtbank echter niet door de Staat worden genegeerd, terwijl uit het oogpunt van nationale veiligheid niet van de Staat kan worden verwacht dat hij de samenwerking met buitenlandse diensten als gevolg van die praktijk ook dan verbreekt als deze diensten op zichzelf voldoen aan de eerder geschetste criteria voor samenwerking. Als eenmaal aan de criteria voor samenwerking wordt voldaan, noopt artikel 8 EVRM niet tot het eerder genoemde "hek aan

de grens". En juist dit vormt de kern in deze procedure voor zover het gaat om de ontvangst en het gebruik van gegevens door de diensten van buitenlandse diensten wanneer deze gegevens zijn verkregen met de inzet van bevoegdheden waarover de Nederlandse diensten niet beschikken, waaronder met behulp van 'PRISM' of vergelijkbare programma's.

5.35. De omstandigheid dat niet kan worden uitgesloten dat, ondanks de internationale verdragsverplichtingen en de nationale wet- en regelgeving waaraan de desbetreffende buitenlandse diensten zijn gebonden, de diensten gegevens verwerven die in het buitenland zijn verzameld op een wijze die niet in overeenstemming is met artikel 8 EVRM, doet hieraan geen afbreuk. In dit verband is van belang dat 'eenieder' in Nederland verschillende wegen kan bewandelen om, desgewenst, de ontvangst en het gebruik van gegevens door de diensten die afkomstig zijn van (bepaalde) buitenlandse diensten te redresseren. Het CTIVD is een onafhankelijk toezichtsorgaan dat toezicht houdt op de rechtmatigheid van de uitvoering van de Wiv 2002 en de Wet veiligheidsonderzoeken. Zij beschikt voor de uitvoering van haar wettelijke taak over verregaande bevoegdheden, waarbij zij toegang heeft tot alle relevante informatie van de AIVD en de MIVD. Zij heeft voorts de bevoegdheid alle medewerkers van de diensten te horen, getuigen (onder ede) of deskundigen te horen en plaatsen te betreden. Ook kan zij werkzaamheden aan deskundigen opdragen, indien een goede taakuitvoering dit noodzakelijk maakt. Niet alleen verricht de CTIVD in het kader van haar toezichthoudende taak onderzoeken, waarvan zij rapport uitbrengt, zij kan ook de betrokken ministers gevraagd en ongevraagd adviseren over haar bevindingen en heeft ook tot taak te adviseren over de afhandeling van klachten over de diensten. Het CTIVD is, met andere woorden, bij uitstek een geschikt orgaan om in algemene zin, dan wel in een concrete situatie, de geoorloofdheid van de ontvangst en het gebruik van gegevens door de diensten te beoordelen. De geoorloofdheid van het bestuurlijk handelen van de diensten kan voorts aan de Nationale ombudsman ter beoordeling worden voorgelegd. Het externe toezicht op de bevoegdheidsuitoefening zal (achteraf) in voorkomende gevallen kunnen plaatsvinden door de burgerlijke rechter indien een belanghebbende van oordeel is dat er een onrechtmatige daad is gepleegd. De *modus operandi* is dus, anders dan eisers stellen, geen vrijbrief of "absoluut verschoningsrecht" voor het handelen van diensten bij het verwerven van gegevens van buitenlandse diensten.

5.36. Zoals eisers aanvoeren, is in de uitspraak van EHRM 22 november 2012, app. no. 39315/06 (*Telegraaf Media Nederland Landelijke Media B.V. and others v. The Netherlands*) geoordeeld dat de Wiv 2002 niet in "*accordance with the law*" is omdat niet is voorzien in een rechterlijke toets voorafgaand aan de inzet van bijzondere bevoegdheden tegen journalisten om hun journalistieke bronnen te achterhalen. In die zaak was evenwel voldoende aannemelijk dat de journalisten van *De Telegraaf* op basis van de inzet van een daartoe strekkende bijzondere bevoegdheid werden afgeluisterd door de AIVD. Bovendien had het in die zaak (in de nationale procedure) gevorderde gebod tot het staken van alle onderzoeken en het gebruik van bijzondere bevoegdheden door de AIVD, uitsluitend betrekking op de desbetreffende journalisten. Dit nu is in deze zaak anders. Eisers hebben, anders dan een algemene beschrijving van hun activiteiten, geen feiten gesteld waaruit enige concrete aanwijzing blijkt dat met betrekking tot hen persoonlijk gegevens door de diensten zijn ontvangen en gebruikt die zijn verzameld door buitenlandse diensten in strijd met artikel 8 EVRM. De gevorderde verklaring voor recht en het gevorderde gebod de ontvangst en het gebruik van gegevens van buitenlandse diensten te staken, hebben verder niet slechts betrekking op eisers, maar zijn algemeen van aard.

5.37. Gelet op dit alles is de enkele omstandigheid dat rekening moet worden gehouden met de mogelijkheid dat de diensten gegevens ontvangen en gebruiken die door de buitenlandse diensten zijn verzameld op een wijze die niet in overeenstemming is met artikel 8 EVRM, onvoldoende voor de conclusie dat, bij gebreke aan de door eisers gestelde waarborgen in de Wiv 2002, de ontvangst en het gebruik door de diensten van gegevens afkomstig van buitenlandse diensten die zijn vergaard met de inzet van bevoegdheden waarover de diensten zelf niet beschikken onder alle omstandigheden in strijd met artikel 8 EVRM is.

5.38. De rechtbank verwerpt tevens de stelling van eisers dat de Wiv 2002 niet voldoet aan de hiervoor in 5.25. genoemde tweede en derde vereisten, die nopen tot een onderzoek naar de vraag in hoeverre de inmenging een legitiem doel dient en noodzakelijk is in een democratische samenleving. Blijkens de rechtspraak van het EHRM komt de nationale autoriteiten een ruime beoordelingsvrijheid (*“wide margin of appreciation”*) toe inzake de vraag of een gerechtvaardigd belang door de inmenging gediend is (zie o.a. in de eerdergenoemde uitspraak in *Weber and Saravia v. Germany*, par. 106). Dat de nationale veiligheid op zichzelf een voldoende legitiem doel is om in het kader van internationale samenwerking mede gegevens afkomstig van buitenlandse diensten te verwerven, is niet in geschil. Om te kunnen voldoen aan het noodzakelijkheids criterium moet sprake zijn van een dringende maatschappelijke behoefte (*“pressing social need”*) en worden voldaan aan het vereiste van proportionaliteit (*“proportionate to the legitimate aim pursued”*). Volgens eisers valt niet in te zien waarom het noodzakelijk is dat de diensten de beschikking krijgen over gegevens die de buitenlandse diensten verkregen hebben door een schending van grondrechten en deze gegevens gebruiken. De Staat moet volgens eisers aantonen waarom niet naar de herkomst van informatie kan worden geïnformeerd en waarom de samenwerking niet op een minder ingrijpende manier kan. Niet aan de orde is evenwel de vraag of het noodzakelijk is om gegevens te verkrijgen die in strijd met artikel 8 EVRM zijn verworven. Het gaat om een dringende maatschappelijke behoefte dat met buitenlandse diensten wordt samengewerkt en dat in dat verband verzamelingen gegevens in bulk worden uitgewisseld. Zoals de Staat ter zitting naar voren heeft gebracht, kan wel naar de herkomst van informatie worden geïnformeerd, maar zal daarop in de regel geen antwoord worden gegeven. Dat, als een partner eenmaal aan de voor samenwerking geldende criteria voldoet, de aard en inhoud van die samenwerking, op voorhand niet zijn beperkt, is ook gerechtvaardigd gelet op de risico's voor de nationale veiligheid die aan een andere benaderingswijze zouden kunnen zijn verbonden. Van de Staat kan niet worden gevergd dat hij de dringend noodzakelijke samenwerking met buitenlandse diensten, zoals die van de VS, op het spel zet louter op grond van onbekendheid met hun werkwijze en de kans dat de Nederlandse diensten informatie ontvangen die is vergaard op een in Nederland niet toegelaten wijze. Het zwaarwegende belang van de nationale veiligheid geeft hier de doorslag.

5.39. De Snowden-onthullingen en het rapport van de CTIVD van 5 februari 2014 zijn aanleiding voor de Staat om (conform de aanbeveling van het CTIVD) de samenwerkingsrelaties (ook in internationaal verband) te beoordelen op transparantie en om de afwegingen die daaraan ten grondslag liggen nader te concretiseren. In dat verband zal ook artikel 59 Wiv 2002 worden aangepast. De rechtbank acht deze omstandigheden niet van belang voor haar beoordeling. Heroverweging van de samenwerking en aanpassing van de regelgeving zeggen immers op zichzelf niets over de rechtmatigheid van die samenwerking en regelgeving tot nog toe. Hetzelfde geldt voor de aanbevelingen van de

---

Committee on Civil Liberties, Justice and Home affairs. Het aandrigen op de naleving van artikel 8 EVRM impliceert niet dat die bepaling niet nageleefd wordt.

5.40. Voor zover eisers zich ten slotte nog beroepen op de Dataprotectierichtlijn en de uitspraak van het Europese Hof van Justitie van 8 april 2014 over de Dataretentierichtlijn, verwerpt de rechtbank dit beroep. Deze richtlijnen zijn niet van toepassing op kwesties betreffende nationale veiligheid. In deze zaak is overigens niet aan de orde of de Wiv 2002 uit het oogpunt van de bescherming van persoonsgegevens voldoet aan de betreffende richtlijnen.

5.41. Het beroep op schending van artikel 8 EVRM en de artikelen 7 en 8 van het Handvest faalt op grond van al het vorenstaande. Nu eisers geen zelfstandige gronden hebben aangevoerd voor hun beroep op schending van artikel 10 EVRM en de door hen genoemde bepalingen in het IVBPR, faalt het beroep op schending van die bepalingen eveneens. Hieruit vloeit voort dat evenmin sprake is van schending van de Wiv 2002. Van onrechtmatig handelen van de Staat wegens schending van de Wiv 2002 en/of internationale verdragsverplichtingen, zoals eisers stellen, is geen sprake.

*Positieve verplichting?*

5.42. Met betrekking tot de door eisers gestelde schending door de Staat van een uit artikel 8 EVRM voortvloeiende positieve verplichting om alle mogelijke passende maatregelen te treffen om de persoonlijke levenssfeer en communicatievrijheid van haar burgers te beschermen, overweegt de rechtbank als volgt.

5.43. Een positieve verplichting voor de Staat om in het kader van de internationale samenwerking bij de buitenlandse diensten steeds navraag te doen naar de wijze van vergaring van gegevens en burgers in de gelegenheid te stellen om te verifiëren of op ongeoorloofde wijze informatie over hen is vergaard en indien dit het geval is deze gegevens te wissen, vloeit niet voort uit het recht op bescherming van de persoonlijke levenssfeer zoals in artikel 8 EVRM neergelegd. Uit hetgeen hiervoor is overwogen in verband met artikel 59 Wiv 2002, blijkt dat de Staat niet verplicht is om voorafgaand aan de ontvangst van gegevens te informeren naar de wijze waarop gegevens door een buitenlandse dienst zijn verzameld. Uit artikel 8 EVRM vloeit evenmin een algemene informatieverplichting of verplichting tot vernietiging van gegevens, zoals eisers voorstaan, voort. Blijkens de rechtspraak van het EHRM valt een weigering van de nationale autoriteiten om toegang te verschaffen tot bepaalde persoonsgegevens binnen het toepassingsbereik van artikel 8 EVRM (vgl. eerdergenoemde uitspraak van het EHRM in de zaak *Leander v. Sweden*, par. 48). Dit laat onverlet dat in artikel 8 EVRM geen algemeen recht op toegang tot (persoons)gegevens is neergelegd, maar dat aan de hand van de concrete omstandigheden van het geval moet worden beoordeeld of een recht op toegang bestaat (zie EHRM 7 juli 1989, app. no. 10454/83, *Gaskin v. The United Kingdom*, par. 37). Voorts kan uit artikel 8 EVRM in het geval van geheime surveillance geen absolute notificatieverplichting achteraf worden afgeleid, aangezien dat praktisch onuitvoerbaar zou zijn (zie EHRM 6 september 1978, app. no 5029/71 (*Klass v. Germany*), par. 58).

5.44. De rechtbank stelt verder vast dat de artikelen 47 en 51 Wiv 2002 een kennisgevingsregeling behelzen en dat in artikel 43 Wiv 2002 is bepaald wanneer gegevens worden verwijderd en vernietigd.

5.45. Eisers hebben ten slotte geen feiten en omstandigheden gesteld waaruit volgt dat ten aanzien van henzelf, dan wel van de personen voor wie zij opkomen sprake is van een concrete inbreuk op het recht op bescherming van de persoonlijke levenssfeer door het ontvangen en gebruiken van gegevens die buitenlandse diensten, in het bijzonder de NSA, aan de diensten hebben verstrekt.

5.46. Gelet op het vorenstaande faalt de stelling van eisers dat op de Staat een positieve verplichting rust om hen te informeren en gegevens te wissen in de zin zoals door hen gesteld.

*Slotsom*

5.47. Het gaat in deze zaak om de verhouding tussen de zwaarwegende belangen (van individuen en van “eenieder”) waarvoor eisers opkomen en het eveneens zwaarwegende algemene belang van internationale samenwerking ten behoeve van de nationale veiligheid. Daarbij is de vraag aan de orde of de Staat (AIVD en MIVD) tegenover eisers onrechtmatig handelt door het ontvangen en het eventueel gebruiken van gegevens van buitenlandse diensten die zijn vergaard op een wijze die mogelijk in strijd is met de hier geldende regels van verdragen en de nationale wetgeving (Wiv 2002). De vorderingen zijn algemeen geformuleerd en gaan uit van de gedachte dat reeds de mogelijkheid dat dit het geval is, een onrechtmatige daad jegens eisers oplevert.

5.48. De rechtbank stelt vast dat inderdaad de *mogelijkheid* bestaat dat de Nederlandse diensten kabelgebonden informatie ontvangen en gebruiken die door buitenlandse diensten, elders, “ongericht” is vergaard. De Nederlandse diensten hebben zelf niet de bevoegdheid dergelijke gegevens te vergaren. De rechtbank heeft deze handelwijze van de Nederlandse diensten getoetst aan onder meer de Wiv 2002 en artikel 8 EVRM. De ontvangst van de gegevens waarover het hier gaat, vindt plaats op basis van artikel 59 lid 1 Wiv 2002, dat bepaalt dat de diensten verbindingen onderhouden met buitenlandse diensten en dat derhalve uitgaat van de geoorloofdheid van contacten met andere diensten. De Nederlandse diensten mogen, op zichzelf bezien, dus samenwerken met de VS en daarmee ook gegevens afkomstig uit de VS ontvangen en gebruiken. Deze staat is gebonden aan eigen regelgeving, die in algemene zin gezegd niet strijdig is met de eisen van artikel 8 EVRM. In sommige opzichten biedt die regelgeving echter minder waarborgen ten opzichte van degenen die geen staatsburger van de VS zijn. Dit leidt tot de vraag hoe het ontvangen en vervolgens gebruiken van elders vergaarde informatie die de diensten niet zelf met de inzet van bijzondere bevoegdheden op grond van de Wiv 2002 hadden mogen verzamelen, zich verhoudt tot de waarborgen op grond van artikel 8 EVRM.

5.49. De rechtspraak van het EHRM over de reikwijdte van dit artikel heeft geen betrekking op het ontvangen en het gebruiken van gegevens die zijn verkregen in het kader van internationale samenwerking met staten die, zoals de VS, in algemene zin als betrouwbare samenwerkingspartners worden gezien. De rechtbank heeft de werkwijze van de Staat getoetst aan de algemene eisen van artikel 8 EVRM, die inhouden dat inbreuken op het daarin vastgelegde grondrecht een basis moeten hebben in de nationale wetgeving en voorzienbaar zijn, en voorts noodzakelijk dienen te zijn in een democratische samenleving voor de verwezenlijking van doeleinden zoals de nationale veiligheid. Daarbij gelden voor het onderscheppen van (ruwe) gegevens in bulk zonder dat deze op relevantie zijn beoordeeld - hetgeen in deze procedure centraal staat - minder strikte eisen dan voor het kennismaken van de inhoud van de communicatie. Er is bovendien een relevant onderscheid

tussen het ontvangen van gegevens en het vervolgens gebruikmaken van die gegevens in individuele gevallen. De rechtbank concludeert dat, in deze context, aan de hier beschreven eisen is voldaan. Gegeven het uitgangspunt van artikel 59 lid 1 Wiv 2002 en de ruime beoordelingsvrijheid van de lidstaten bij de toetsing aan artikel 8 EVRM, betoogt de Staat op toereikende gronden dat van hem niet kan worden gevergd dat hij de dringend noodzakelijke samenwerking met buitenlandse diensten, zoals die van de VS, op het spel zet louter op grond van onbekendheid met hun werkwijze en de kans dat de Nederlandse diensten informatie ontvangen die is vergaard op een in Nederland niet toegelaten wijze. Het zwaarwegende belang van de nationale veiligheid geeft hier de doorslag.

5.50. De zwaarwegende belangen van eisers zullen op individuele basis tot hun recht moeten komen in de waarborgen die de Wiv 2002 biedt of toelaat in geval van gebruik in hun nadeel, te weten een beroep op de CTIVD, op de Nationale ombudsman of - in bijzondere gevallen, indien aan de desbetreffende voorwaarden is voldaan - op de nationale civiele of bestuursrechter.

5.51. Tot slot brengt artikel 8 EVRM niet mee dat op de Staat een positieve verplichting rust om betrokkenen te informeren en gegevens te wissen zoals eisers stellen.

5.52. Voor toewijzing van de algemeen geformuleerde vorderingen bestaat geen grond.

#### **Proceskosten**

5.53. Eisers zullen als de in het ongelijk gestelde partij worden veroordeeld in de kosten van de procedure aan de zijde van de Staat. Die kosten worden tot op heden begroot op € 1.493,- (€ 589,- aan griffierecht en € 904,- aan salaris advocaat; twee punten volgens tarief II (€ 452,-), dat onder meer in zaken van onbepaalde waarde wordt gebruikt).

#### **6. De beslissing**

De rechtbank:

6.1. wijst de vorderingen af;

6.2. veroordeelt eisers in de kosten van de procedure aan de zijde van de Staat, tot op heden begroot op € 1.493,-;

6.3. verklaart deze proceskostenveroordeling uitvoerbaar bij voorraad.

Dit vonnis is gewezen door mr. H.F.M. Hofhuis, mr. M.J. Alt-van Endt en mr. M.C. Ritsema van Eck-van Drempt en in het openbaar uitgesproken op 23 juli 2014.